View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repositorio Institucional UniLibre

VPNS A TRAVÉS DEL PROTOCOLO IPSEC Y ADMINISTRACIÓN DE SEGURIDAD EN ROUTERS CISCO

CAMILO ANTONIO RODRIGUEZ RODRIGUEZ

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERIA

BOGOTA

2011

VPNS A TRAVÉS DEL PROTOCOLO IPSEC Y ADMINISTRACIÓN DE SEGURIDAD EN ROUTERS CISCO

CAMILO ANTONIO RODRIGUEZ RODRIGUEZ

PROYECTO DE GRADO PRESENTADO COMO REQUISITO PARA OBTENER EL TITULO DE INGENIERO DE SISTEMAS

DIRECTOR:

BEATRIZ ALEXANDRA ARBELAEZ HURTADO

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERIA

BOGOTA – 2011

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____

_____

Jurado

_____

Jurado

Bogota D.C

DEDICATORIA

Este trabajo, esta dedicado a mi esposa **Magda** por ese apoyo incondicional, por sus palabras de animo y por todo el amor que me da como amiga y pareja, a mi **madre**, por su presencia y cariño, por llevarme en su vientre y traerme al mundo y por ese amor, que solo una madre puede dar, un amor que va mas allá de las fronteras, del bien y del mal y de la vida misma, a mi **padre** quien gracias a su apoyo y ayuda tuve la oportunidad de realizar una carrera profesional, a mi **hermana**, por su amor inocente, su cariño, firmeza y por ese ángel que la acompaña ante las mas grandes dificultades de la vida.

A mis **profesores**, quienes me han enseñado y me han guiado con paciencia, amabilidad y camaradería por la senda del conocimiento propio y profesional.

A **Dios**, pintor del universo el cual lo plasmo en el lienzo de las matemáticas, padre y dueño de mi vida y de mi espíritu.

A la **vida** que me ha llevado por diversos senderos de enseñanza y autoconocimiento.

AGRADECIMIENTOS

Mi mas sincero y profundo agradecimiento a la Universidad Libre, a mis profesores y compañeros de carrera, con los cuales compartí muchas experiencias enriquecedoras en el campo profesional y personal, a su apoyo, amistad y paciencia.

CONTENIDO

Pag.

Pag.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pág.

RESUMEN

Se realizo un trabajo teórico-experimental del funcionamiento de las VPNs a través del protocolo IPSec basado en entornos CISCO, en el cual se realizo un modelo detallado al trabajo de investigación realizado, esta aplicación se desarrollo bajo la plataforma Cisco Packet Tracer® el cual simula un entorno de red y el funcionamiento de este como lo haría en un ambiente real.

Esta investigación arrojo unos resultados satisfactorios, el protocolo IPSec (IP Security – Seguridad IP) es un protocolo sencillo de implementar y configurar, y muy confiable a la hora de permitir una comunicación en red por medio de VPNs (Virtual Private Networks – Redes Privadas Virtuales).

IPSec es un protocolo que permite implementar y configurar VPNs pues proporciona diversos servicios de seguridad tanto para IPv4 e IPv6.

VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Existen varios tipos de VPN, la más usada es la VPN de acceso remoto, la cual consiste de varios usuarios o proveedores que se conectan a los datos de la empresa de forma remota, utilizando internet como medio de acceso, lo cual conlleva unas ventajas como la integridad y la confidencialidad de los datos la reducción de costos, la sencillez en la instalación de la VPN en un equipo cliente y su fácil uso y el control del acceso basado en las políticas de la empresa.

La implementación y configuración de una VPN proporciona un servicio de seguridad a través de los routers y la plataforma tecnológica, al querer tener disponibilidad de los datos desde cualquier punto para acceder de forma segura y confiable.

ABSTRACT

We performed a theoretical and experimental work performance of VPNs over IPSec-based Cisco environments in which we made a detailed implementation research work, this application was developed under the Cisco Packet Tracer® platform which simulates a network environment and operation of this as you would in a real environment.

This research indicated a satisfactory outcome, the IPSec protocol is a simple protocol to implement and configure, and very reliable in enabling a communication network via VPNs.

IPSec is a protocol that allows you to deploy and configure VPNs as it provides various security services for both IPv4 and IPv6.

A virtual private network or VPN is a networking technology that allows an extension of the local network over a public network or not controlled, such as Internet.

Common examples are the ability to connect two or more branches of a company using Internet as a link, to enable team members support the link from its home at the computer center, or a user can access from your home computer a remote site, such as a hotel. All using the Internet infrastructure.

There are several types of VPN, the most used is the remote access VPN, which consists of multiple users or providers who connect to corporate data remotely, using internet as a means of access, which are advantages as integrity and confidentiality of data cost reduction, simplicity in installing the VPN client on a computer and easy to use and access control based on company policies.

The implementation and configuration of a VPN provides a security service to routers and the network itself, wanting to have use of data from any access point that must be safely and reliably.

PALABRAS CLAVE

VPN – Cisco – Red – IPSec – Protocolo

1. INTRODUCCIÓN

1.1 PROBLEMA

¿Se perfecciona el acceso a la información de forma oportuna, segura, confiable y confidencial por parte de los usuarios de una red con la implementación de VPNs por medio del protocolo IPSec?

La Tecnología de acceso remoto a la información por medio de la implementación de las VPNs a través del protocolo de seguridad IPSec basado en entornos de red CISCO ofrece una alternativa útil y eficaz para mejorar el funcionamiento de una red y la disponibilidad de la información que fluye a través de ella la cual puede ser requerida por parte de aquellos usuarios que trabajan mas allá de los limites en los cuales la red funciona como alternativa para tener acceso a la información.

1.4 OBJETIVOS

1.4.1 Objetivo general:

Dar a conocer a través de un documento técnico la implementación y el funcionamiento de las *VPNs* en entornos Cisco a través del protocolo *IPSec*.

1.4.2 Objetivos Específicos:

- Establecer el concepto teórico y técnico del Protocolo IPSec y su aplicación en la Administración de Seguridad de Routers
- Identificar como se implementa y configura una VPN por medio del protocolo IPSec en Routers Cisco
- Definir como se planifica la Administración de Seguridad de los Routers Cisco

1.5 DELIMITACIÓN

1.5.1 Delimitación espacial: Esta investigación se limito a ser verificada en el laboratorio de Hardware y Redes de la Universidad Libre, por medio de una practica de laboratorio en la que se creo y configuro una *VPN* por medio del protocolo *IPSec*.

1.5.2 Delimitación Temática: El tema que abarca esta investigación es la de Networking y Seguridad en Redes.

1.5.3 Delimitación Técnica: Se utilizaron los procesos de creación y configuración de VPNs desarrolladas por CISCO para la aplicación de la investigación realizada.

1.6 JUSTIFICACION

En la actualidad la globalización y la competencia hacen que las empresas, estén cada vez mas al día y actualizadas en el funcionamiento, mejoramiento y manejo eficiente de sus activos tecnológicos y de la información que fluye a través de esta, muchas empresas crecen y se expanden, lo que hace que ya no sea una oficina central la que maneje toda la información, y se creen pequeñas células o sucursales, las cuales necesitan tener acceso a la información de la empresa como si estuvieran en la oficina principal, o algunas empresas no cuentan con una planta física lo suficientemente grande, como para agrupar a todos sus empleados en un mismo sitio generando así la figura de un trabajador a distancia que puede laborar desde su hogar o desde una oficina tipo sucursal. Debido a estas limitaciones espaciales, se hace necesario adoptar una tecnología de acceso remoto a la información por parte de las sucursales y *Teleworkers* (Trabajadores a distancia) de la empresa que sea segura y confiable y que le permita a estos usuarios tener acceso a la información de forma oportuna. El uso de las *VPNs* (Redes Privadas Virtuales) a través del protocolo IPSec en entornos de red basados en Cisco es una de las alternativas mas comunes que utilizan las empresas debido a que esta es una tecnología que ofrece una conexión remota entre una sucursal y su oficina principal, o entre un trabajador a distancia y una oficina principal de forma segura, confiable y confidencial, lo que permite tener un acceso oportuno y eficiente a la información requerida.

Es necesario conocer el funcionamiento del protocolo IPSec, como alternativa ofrecida por los sistemas de red Cisco como protocolo que ofrece la creación de VPNs basadas en seguridad, confiabilidad y confidencialidad garantizadas.

No hay que olvidar que el protocolo IPSec es uno de los protocolos de seguridad de red basado en paquetes IP más importante, robusto y efectivo a la hora de evitar violaciones de seguridad, falsificación de la información y el robo de la misma.

De esta forma se están abriendo las puertas a conocer y profundizar en una tecnología relativamente nueva que esta revolucionando las redes y el acceso a las mismas de forma remota pero segura.

Los estudiantes de la universidad, podrían disfrutar de una información confiable, de una investigación que se centra en una temática poco explorada, y que podría servir como semillero de investigación para nuevos trabajos y para profundizar en un tema tan extenso como es el acceso remoto y la seguridad en redes.

2. MARCO TEÓRICO

2.1 TCP/IP

Las siglas *TCP/IP* se refieren a dos protocolos de red, que son *Transmission Control Protocol* (Protocolo de Control de Transmisión) e *Internet Protocol* (Protocolo de Internet) respectivamente. Estos protocolos pertenecen a un conjunto mayor de protocolos. Dicho conjunto se denomina suite TCP/IP.

Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedamos a los distintos servicios de la Red. Como el acceso a la World Wide Web, acceso al correo electrónico, generadores de noticias *RSS (Rich Site Summary – Sindicación de Contenidos de Paginas Web)* etc.

Hay dos clases de protocolos dentro de la suite TCP/IP que son: protocolos a nivel de red y protocolos a nivel de aplicación.

2.1.1 Protocolos a Nivel de Red: Estos protocolos se encargan de controlar los mecanismos de transferencia de datos. Normalmente son invisibles para el usuario y operan por debajo de la superficie del sistema. Dentro de estos protocolos tenemos:

TCP. Controla la división de la información en unidades individuales de datos (llamadas paquetes) para que estos paquetes sean encaminados de la forma más eficiente hacia su punto de destino. En dicho punto, TCP se encargará de reensamblar dichos paquetes para reconstruir el fichero o mensaje que se envió. Por ejemplo, cuando se nos envía un fichero HTML desde un servidor Web, el protocolo de control de transmisión en ese servidor divide el fichero en uno o más paquetes, numera dichos paquetes y se los pasa al protocolo IP. Aunque cada paquete tenga la misma dirección IP de destino, puede seguir una ruta diferente a través de la red. Del otro lado (el programa cliente en nuestro ordenador), TCP reconstruye los paquetes individuales y espera hasta que hayan llegado todos para presentárnoslos como un solo fichero.
IP. Se encarga de repartir los paquetes de información enviados entre el ordenador local y los ordenadores remotos. Esto lo hace etiquetando los paquetes con una serie de información, entre la que cabe destacar las direcciones IP de los dos ordenadores. Basándose en esta información, IP garantiza que los datos se encaminarán al destino correcto. Los paquetes recorrerán la red hasta su destino (que puede estar en el otro extremo del planeta) por el camino más corto posible gracias a unos dispositivos denominados routers.

2.1.2 Protocolos a Nivel de Aplicación: Aquí tenemos los protocolos asociados a los distintos servicios de Internet, como *FTP(File Transfer Protocol – Protocolo de Transferencia de Archivos)*, *Telnet*, *Gopher*, *HTTP (Hyper Text Transfer Protocol – Protocolo de Transferencia de Hipertexto)*, etc. Estos protocolos son visibles para el usuario en alguna medida. Por ejemplo, el protocolo *FTP* (*File Transfer Protocol*) es visible para el usuario. El usuario solicita una conexión a otro ordenador para transferir un fichero, la conexión se establece, y comienza la transferencia. Durante dicha transferencia, es visible parte del intercambio entre la máquina del usuario y la máquina remota (mensajes de error y de estado de la transferencia, como por ejemplo cuantos bytes del fichero se han transferido en un momento dado).

2.1.3 Historia de TCP/IP: A principios de los años 60, varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una forma más eficiente. En 1961, Leonard Klienrock introduce el concepto de Conmutación de Paquetes (Packet Switching, en inglés). La idea era que la comunicación entre ordenadores fuese dividida en paquetes. Cada paquete debería contener la dirección de destino y podría encontrar su propio camino a través de la red.

Como ya comentamos en el capítulo anterior, en 1969 la Agencia de Proyectos de Investigación Avanzada (*Defense Advanced Research Projects Agency* o *DARPA*) del Ejército de los EEUU desarrolla la *ARPAnet*. La finalidad principal de esta red era la capacidad de resistir un ataque nuclear de la URSS para lo que se pensó en una administración descentralizada. De este modo, si algunos ordenadores eran destruidos, la red seguiría funcionando. Aunque dicha red funcionaba bien, estaba sujeta a algunas caídas periódicas del sistema. De este modo, la expansión a largo plazo de esta red podría resultar difícil y costosa. Se inició entonces una búsqueda de un conjunto de protocolos más fiables para la misma. Dicha búsqueda finalizó, a mediados de los 70, con el desarrollo de TCP/IP.

TCP/IP tenia (y tiene) ventajas significativas respecto a otros protocolos. Por ejemplo, consume pocos recursos de red. Además, podía ser implementado a un coste mucho menor que otras opciones disponibles entonces. Gracias a estos aspectos, TCP/IP comenzó a hacerse popular. En 1983, TCP/IP se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la integración en versiones comerciales de UNIX vino pronto. Así es como TCP/IP se convirtió en el estándar de Internet.
En la actualidad, TCP/IP se usa para muchos propósitos, no solo en Internet. Por ejemplo, a menudo se diseñan intranets usando TCP/IP. En tales entornos, TCP/IP ofrece ventajas significativas sobre otros protocolos de red. Una de tales ventajas es que trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden

comunicarse usando la misma suite de protocolos TCP/IP, una vez conocida la historia de TCP/IP veamos como funciona. [1]

2.1.4 Como Funciona TCP/IP: TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se ilustra en la figura siguiente:[2]

Figura 1. Capas Para El Funcionamiento de TCP/IP (Modelo TCP/IP)

Fuente: http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

2.2 CAPA DE APLICACIÓN

La capa de aplicación se encuentra en la parte superior de las capas del modelo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo. Se pueden clasificar según los servicios que brindan:

- Servicios de administración de archivos e impresión (transferencia);
- Servicios de conexión a la red;
- Servicios de conexión remota;
- Diversas utilidades de Internet.[3]

[1] http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm
[2] http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm
[3] http://es.kioskea.net/contents/internet/tcpip.php3

2.3 CAPA DE TRANSPORTE

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones. De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc.

Además, el nombre de la aplicación puede variar de sistema en sistema. Es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son los siguientes:

- *TCP (Transmission Control Protocol – Protocolo de Control de Transmisión)*: Protocolo orientado a la conexión que brinda detección de errores;
- *UDP (User Datagram Protocol – Protocolo de Datagramas de Usuario)*: Protocolo no orientado a la conexión en el que la detección de errores es obsoleta. El protocolo se orienta a transacciones, y tanto la entrega como la protección ante duplicados no se garantizan[4].

2.3.1 Protocolo TCP: El "protocolo de control de transmisión" (Transmission Control Protocol, TCP) está pensado para ser utilizado como un protocolo "host" a "host" muy fiable entre miembros de redes de comunicación de computadoras por intercambio de paquetes y en un sistema interconectado de tales redes[5].

TCP es un protocolo de transporte orientado a conexión enormemente extendido en Internet. Las aplicaciones de red más populares (*ftp*, *telnet*, *acceso Web*…) lo utilizan en sus comunicaciones.

2.3.2 Protocolo UDP: (*User Datagram Protocol*) Protocolo de Datagramas de Usuario, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no

[4] http://www.rfc-es.org/rfc/rfc0768-es.txt
[5] http://www.rfc-es.org/rfc/rfc0793-es.txt

hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP (*Dynamic Host Control Protocol – Protocolo de Control de Host Dinámico*), BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.[6]

2.4 INTERNET

La capa de Internet es la capa "más importante" (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP.

Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben.

La capa de Internet contiene 5 protocolos:

- El protocolo IP (Internet Protocol)
- El protocolo ARP (Address Resolución Protocol)
- El protocolo ICMP (Internet Control Message Protocol)
- El protocolo RARP (Reverse Address Resolution Protocol)
- El protocolo IGMP (Internet Group Management Protocol)

Los primeros tres protocolos son los más importantes para esta capa.[7]

2.4.1 Protocolo IP:

(*Internet Protocol*) Es un protocolo no orientado a la conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas. En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (*best effort*), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante *checksums* o sumas de comprobación) de sus cabeceras y no de los datos

[6] http://es.wikipedia.org/wiki/User_Datagram_Protocol
[7] http://es.kioskea.net/contents/internet/tcpip.php3

transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP, ahora veamos que es el direccionamiento IP y como funciona.[8]

2.5 DIRECCIONAMIENTO IP

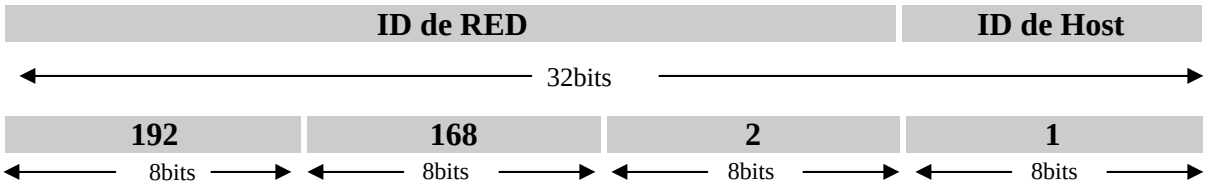
2.5.1 Dirección IP: Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo de Internet (IP) que corresponde al nivel de red o capa 3 del modelo de referencia *OSI* (*Open Systems Interconnection*) "Interconexión de sistemas Abiertos". Dicho número no se ha de confundir con la dirección *MAC* (*Media Access Control*) "Acceso de Control al Medio" que es un número físico que es asignado a la tarjeta o dispositivo de red (impuesta por el fabricante), mientras que la dirección IP se puede cambiar.[9] Existen dos tipos de dirección IP. Dirección IP Dinámica, la cual es la que habitualmente se utiliza cuando nos conectamos a Internet desde casa y esta dirección cada vez que nos conectamos cambia, el protocolo que asigna direcciones IP dinámicas se llama *DHCP* (*Dynamic Host Configuration Protocol*) "Protocolo de Configuración Dinámica de Host". Dirección IP estática la cual se asigna por medio de un servidor de correo o servidores DNS (*Domain Name Server*) "Servidor de Nombres de Dominio", a cada dispositivo en la red se le asigna una y solo una dirección IP y nunca cambia su número.

Una dirección IP es una consecución de 4 números (4 octetos) separados por punto, cada octeto esta conformado por 8 bits, para un total de 32 bits. Ejemplo de una dirección IP seria **192.168.2.1**

2.5.2 Componentes de una dirección IP: Al igual que la dirección de una casa tiene dos partes (una calle y un código postal), una dirección IP también está formada por dos partes: el ID de host y el ID de red.

[8] http://es.wikipedia.org/wiki/Protocolo_IP
[9] http://es.wikipedia.org/wiki/Protocolo_IP

Figura 2. Componentes de una dirección IP



Fuente: http://es.wikipedia.org/wiki/Protocolo_IP

El ID de red identifica el segmento de red en el que esta ubicado el equipo. Todos los equipos en un mismo segmento deben tener el mismo ID de red. El ID de host identifica un equipo, un router, u otro dispositivo en un segmento determinado.[10]

La combinación entre el ID de host y el ID de red debe ser único para cada equipo y dispositivo en la red.

Las direcciones IP están divididas en clases, estas clases se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones IP también se utilizan para definir el punto de de división entre el ID de red y el ID de host.

Figura 3. Clases de Direcciones IP

Clase A	**ID de Red**	**ID de Host**	**ID de Host**	**ID de Host**
Clase B	**ID de Red**	**ID de Red**	**ID de Host**	**ID de Host**
Clase C	**ID de Red**	**ID de Red**	**ID de Red**	**ID de Host**
Clase D	**ID de Host**	**ID de Host**	**ID de Host**	**ID de Host**

Fuente: http://es.wikipedia.org/wiki/Protocolo_IP

Una dirección IP Clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer octeto para el ID de red, los tres restantes se utilizan para el ID de host permitiendo 16.777.214 hosts por red.

[10] http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml#compon

Una dirección IP Clase B se asignan a redes de tamaño mediano a grande, permitiendo 16.384 redes, utilizando los dos primeros números para el ID de red, los dos números restantes se utilizan para el ID de host permitiendo 65.534 hosts por red.

Una dirección IP Clase C se utilizan para redes *LAN* pequeñas (*Local Area Network*) "Redes de Área Local" Esta clase permite 2.097.152 redes utilizando los tres primeros octetos para el ID de Red y dejando el cuarto para el ID de host, permitiendo 254 hosts por red.

Las clases D y E no se asignan a hosts, las direcciones clase D se utilizan para multicast y las direcciones clase E se reservan para uso futuro.[11] Ya conocemos TCP/IP su historia y funcionamiento, Direccionamiento IP, ahora profundicemos mas en el tema de investigación de este trabajo de grado y conozcamos un poco mas sobre el protocolo de seguridad de IP IPSec.

2.6 IPSEC (IP Security – Seguridad IP)

La arquitectura de seguridad para el protocolo IP (*IPSec*) proporciona diversos servicios de seguridad para el trafico en la capa IP, tanto para ambientes IPv4 (IP Versión 4)[12] e IPv6 (IP Versión 6)[13] IPSec está diseñado para proporcionar seguridad ínter-operable, de alta calidad, basada en criptografía tanto para IPv4 como para IPv6. El conjunto de servicios de seguridad ofrecidos incluye: control de acceso, integridad sin conexión, autenticación del origen de los datos, protección antireplay (una forma de integrabilidad parcial de la secuencia), confidencialidad (encriptación), y confidencialidad limitada del flujo de tráfico. Estos servicios se implementan en la capa IP, y ofrecen protección para este nivel y/o los niveles superiores.

Estos objetivos se llevan a cabo haciendo uso de dos protocolos de seguridad, la Cabecera de Autentificación (*AH "Authentication Header"*) y Carga de Seguridad Encapsulada (*ESP "Encapsulating Security Payload"*), a través de procedimientos de manejo de claves criptográficas y protocolos. El conjunto de protocolos IPsec empleados en cualquier conexión, y la forma en que se emplean, serán determinados por la seguridad, y los requerimientos del sistema del usuario, aplicaciones y/o sitios o organizaciones.

---

[11] http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml#compon

[12] IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales

[13] es una nueva versión de IP (Internet Protocol), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoría de dispositivos que acceden a Internet.

2.6.1 Como Trabaja IPSec: IPSec utiliza dos protocolos para proporcionar seguridad al tráfico: la Cabecera de Autentificación (*AH "Authentication Header"*) y la Carga de Seguridad Encapsulada (*ESP "Encapsulating Security Payload"*).

- La Cabecera de Autentificación (AH): Proporciona integridad sin conexión, autentificación del origen de datos, y un servicio opcional de protección antireplay.
- La Carga de Seguridad Encapsulada (ESP): Puede proporcionar confidencialidad (encriptación), y confidencialidad limitada de flujo de tráfico. También puede proporcionar integridad sin conexión, autentificación del origen de datos, y un servicio de protección antireplay. (Uno u otro de estos servicios de seguridad debe ser aplicado siempre que se use ESP.)
- AH y ESP son instrumentos para el control de acceso, basados en la distribución de claves criptográficas y en el manejo de flujo de tráfico concerniente a estos protocolos de seguridad.

Estos protocolos pueden aplicarse solos o en conjunto con otros para proporcionar un conjunto de servicios de seguridad en IPv4 e IPv6. Cada protocolo soporta dos modos de uso: modo transporte y modo túnel. En modo transporte los protocolos proporcionan protección sobre todo a los protocolos de capa superiores; en modo túnel, los protocolos son aplicados a paquetes (a los que se hizo un túnel a través de IP).

Debido a que estos servicios de seguridad usan valores secretos compartidos (claves criptográficas), IPsec se basa en un conjunto de mecanismos separados para que pongan estas claves en su sitio (las claves se utilizan para autentificación/integrabilidad y los servicios de encriptación). Este documento requiere soporte para la distribución manual y automática de claves. Especifica un acercamiento basado en clave pública o clave de Internet (*IKE "Internet Key Exchange"*) para la gestión automática de claves, pero otras técnicas de distribución automatizada de claves pueden ser utilizadas. Por ejemplo, sistemas como Kerberos.[14]

2.6.2 Asociaciones de Seguridad: Una Asociación de Seguridad (*SA "Security Asociation"*) es fundamental para IPSec AH y ESP hacen uso de estas, una función importante de IKE es el establecimiento y el mantenimiento de SAs.

Una Asociación de Seguridad (SA) es una "conexión" unidireccional (simplex) que ofrece servicios de seguridad al tráfico transportado por este. Los servicios de seguridad ofrecidos en una SA son usados por AH o ESP, pero no por ambos. Si ambos (AH y ESP) se aplican a un flujo de tráfico, dos (o más) SAs se crearán para generar la protección de flujo de tráfico. Para asegurar la comunicación bidireccional entre dos hosts, o entre dos security gateway, se requieren dos Asociaciones de Seguridad (uno en cada sentido).

---

[14] http://www.rfc-es.org/rfc/rfc2401-es.txt

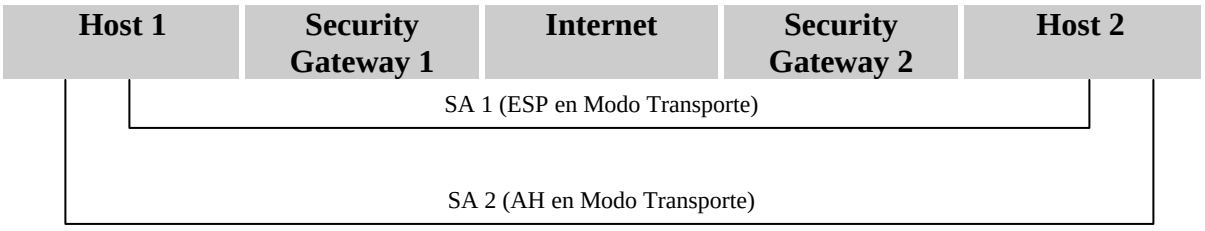
Se definen dos tipos de SAs. Modo Transporte y Modo Túnel. Una SA en modo trasporte es una SA entre dos hosts. Una SA en modo túnel es en esencia una SA aplicada a un túnel IP. Siempre que un extremo de la SA sea un security gateway[15], la SA debe estar en modo túnel. Una SA entre dos security gateway, es siempre una SA en modo túnel, al igual que una SA entre un Host y un security gateway.

2.6.3 Combinación de Asociaciones de Seguridad: Los datagramas IP trasmitidos por una SA individual permiten la protección de un protocolo de seguridad, AH o ESP, pero no ambos. En ocasiones una política de seguridad puede determinar una combinación de servicios para un flujo de tráfico específico que no se puede realizar por una única SA. En estos casos será necesario emplear múltiples SAs para implementar la política de seguridad requerida. El termino "grupo de asociaciones de seguridad" o "grupo de SA" se aplica a una secuencia de SAs las cuales deben procesar el tráfico para satisfacer una política de seguridad.

Las SAs pueden combinarse entre grupos de dos formas: transporte adyacente (*transport adjacency*) y entre túneles (*iterated tunneling*).

- Transporte adyacente: se aplica más de un protocolo de seguridad sobre el mismo datagrama IP, sin utilizar túneles. Este método combina a AH y a ESP permitiendo solamente un nivel de combinación, el anidado adicional no produce un beneficio adicional (asumiendo el uso de algoritmos adecuados en cada protocolo) puesto que el proceso se realiza en una instancia de IPSec en el (último) destino.

Figura 4. Asociación de Seguridad en Modo Transporte



Fuente: http://www.rfc-es.org/rfc/rfc2401-es.txt

- Entre túneles: se refiere a la aplicación de múltiples capas del protocolo de seguridad efectuando múltiples túneles IP. Este método permite múltiples niveles de anidado, puesto que cada túnel se puede originar o terminar en

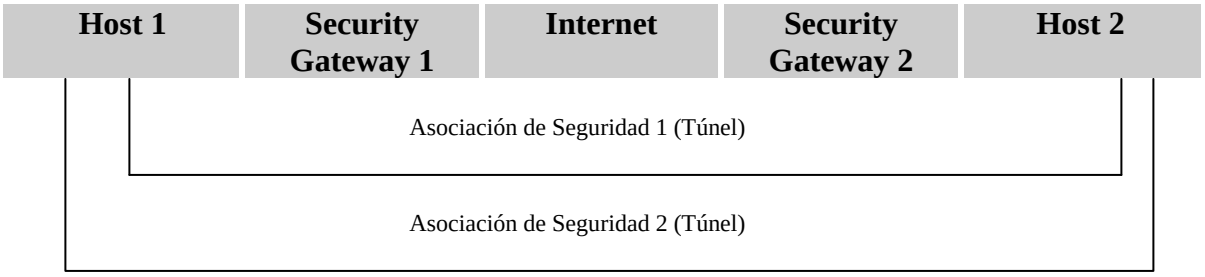
[15] Un Security Gateway, es un dispositivo de red como un router que funciona como Gateway para esa red.

nodos diferentes a lo largo de la trayectoria. No se espera ningún tratamiento especial para el tráfico de ISAKMP[16]

Hay tres casos básicos de entre túneles:

- Ambos extremos de las SAs son los mismos: Los túneles (interno o externo) pueden ser AH o ESP, aunque es improbable que el host 1 especifique ambos túneles iguales, es decir, AH a dentro de AH, o ESP dentro de ESP.

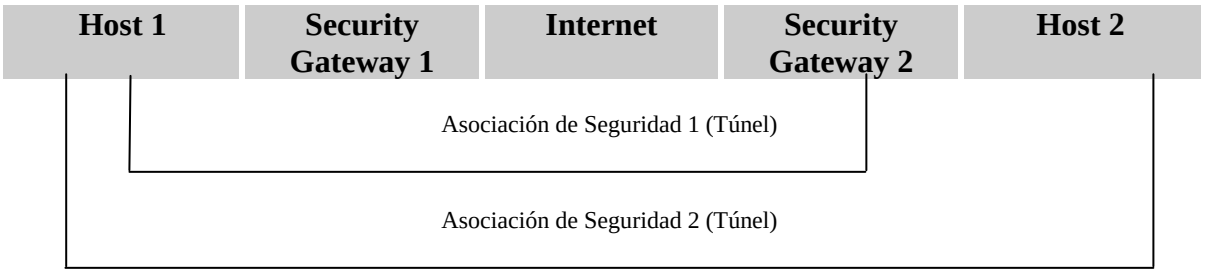
Figura 5. Asociación de Seguridad Modo Túnel 1



Fuente: http://www.rfc-es.org/rfc/rfc2401-es.txt

- Un extremo de las SAs es igual: Los túneles (interno o externo) pueden ser AH o ESP.

Figura 6. Asociación de Seguridad Modo Túnel 2

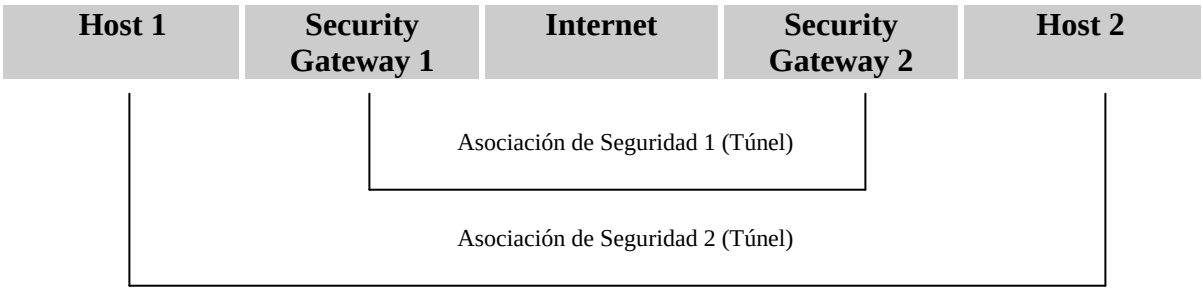


Fuente: http://www.rfc-es.org/rfc/rfc2401-es.txt

[16] Internet Security Association and Key Management Protocol (ISAKMP) es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Está definido en el RFC 2408

- Ninguno de los extremos es igual: Los túneles (interno o externo) pueden ser AH o ESP

Figura 7. Asociación de Seguridad Modo Túnel 3



Fuente: http://www.rfc-es.org/rfc/rfc2401-es.txt

2.7 AH (Authentication Header)

La Cabecera de Autentificación IP (*AH "Authentication Header"*) se usa para proporcionar integridad sin conexión y autenticación del origen de datos para datagramas IP, y para proporcionar protección contra reenvíos. Este último servicio es opcional y puede seleccionarse una vez que se ha establecido la Asociación de Seguridad (SA)[17].

Figura 8. Formato Cabecera Autenticación (AH)

Cabecera Siguiente	**Longitud de carga**	**RESERVADO**
Índice de Parámetros de Seguridad (SPI)		
Número de Secuencia		
Datos de Autentificación (Longitud Variable)		

Fuente: http://www.rfc-es.org/rfc/rfc2402-es.txt

2.8 ESP (Encapsulating Security Payload)

La cabecera de Carga de Seguridad Encapsulada (ESP) esta diseñada para proporcionar un conjunto de servicios de seguridad en IPv4 y en IPv6. ESP puede ser aplicado solo, o en combinación con la Cabecera de Autentificación (AH). ESP es usado para proporcionar

[17] http://www.rfc-es.org/rfc/rfc2402-es.txt

confidencialidad, autentificación del origen de los datos, integridad sin conexión, un servicio de anti-replay (una forma parcial de integrabilidad de secuencia) y confidencialidad limitada del flujo de trafico.[18]

Figura 9. Formato Carga de Seguridad Encapsulada (ESP)

Índice de Parámetros de Seguridad (SPI)	
Numero de Secuencia	
Datos de la Carga Útil (Longitud Variable)	
Relleno (entre 0-255 bytes)	
Longitud de Relleno	**Siguiente Cabecera**
Datos de Autentificación (Longitud Variable)	

Fuente: http://www.rfc-es.org/rfc/rfc2406-es.txt

2.9 IKE (Internet Key Exchange)

El intercambio de claves de Internet (IKE) es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPSec. IKE emplea un intercambio secreto de claves de tipo Diffie-Hellman[19] para establecer el secreto compartido de la sesión. Se suelen usar sistemas de clave pública o clave pre-compartida.

Supone una alternativa al intercambio manual de claves. Su objetivo es la negociación de una Asociación de Seguridad para IPSEC. Permite, además, especificar el tiempo de vida de la sesión IPSEC, autenticación dinámica de otras máquinas, etc.[20]

[18] http://www.rfc-es.org/rfc/rfc2406-es.txt

[19] (Creado por Whitfield Diffie y Martin Hellman) permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.

[20] http://es.wikipedia.org/wiki/Internet_key_exchange

3. VPN (Virtual Private Network)

Una red privada virtual o VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

3.1 TIPOS DE VPN

3.1.1 VPN de acceso remoto: Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

3.1.2 VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

3.1.3 Tunneling: La técnica de tunneling consiste en encapsular un protocolo de red sobre otro creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

3.1.4 VPN over LAN: Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAC Address, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna.[21]

[21] http://es.wikipedia.org/wiki/VPN

3.2 VENTAJAS DE LAS VPN

Dentro de las ventajas más significativas podremos mencionar:

- La integridad.
- Confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC.
- Control de Acceso basado en políticas de la organización.
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

3.3 TIPOS DE CONEXIÓN

3.3.1 Conexión de acceso remoto: Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

3.3.2 Conexión VPN router a router: Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

3.3.3 Conexión VPN firewall a firewall: Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.[22] Las VPNs son parte fundamental de la conexión segura entre redes, por tal motivo ahora veamos un poco sobre administración de seguridad en routers.

[22] http://es.wikipedia.org/wiki/VPN

4. ADMINISTRACIÓN DE LA SEGURIDAD EN ROUTERS CISCO

4.1 EL ROL DE LOS ROUTERS EN LAS REDES MODERNAS

En una red pequeña de computadoras, es factible utilizar mecanismos de difusión simple o secuencial para mover datos de punto a punto. Una red de área local (LAN) es esencialmente una red de difusión. En redes más grandes y complejas, los datos deben ser dirigidos específicamente al destino previsto. Los Routers envían los mensajes de una red o paquetes de datos, basado en las direcciones internas y las tablas de enrutamiento o por destinos conocidos que sirven a ciertas direcciones. Enviar datos entre partes de una red es el objetivo principal de un router.[23]

4.2 MOTIVACIONES PARA PROPORCIONAR UN SERVICIO DE SEGURIDAD EN LOS ROUTERS

Los Routers proveen de una prestación de servicios que son esenciales para el funcionamiento correcto y seguro de las redes que sirven. Comprometer la seguridad de un Router puede dar lugar a diversos problemas de seguridad en la red en la que sirve este router, o incluso otras redes con la que se comunica.

- Comprometer las tablas de enrutamiento de un Router puede resultar en la reducción del rendimiento, la negación de los servicios de comunicación de la red, y la exposición de datos sensibles.
- Comprometer el control de acceso a un router puede resultar en la exposición de detalles de configuración de red o de denegación de servicio, y puede facilitar los ataques contra otros componentes de la misma.
- Una configuración de filtro de Router deficiente puede reducir la seguridad general de un enclave completo, exponer los componentes de la red interna a realizar exploraciones y ataques, y que sea más fácil para los piratas evitar la detección.
- Por otro lado, el uso adecuado de las funciones criptográficas de un Router funciones de seguridad criptográfica puede ayudar a proteger los datos sensibles, garantiza la integridad de los datos, garantiza y facilitar la cooperación entre los enclaves independientes.

---

[23] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

En general, Un Router bien configurado puede mejorar la postura de seguridad global de una red. Una política de seguridad aplicada a un router hace difícil para los usuarios o atacantes negligentes o maliciosos eludir la seguridad de la red, evitando así una posible fuente de problemas de seguridad muy graves.

Hay recursos de seguridad disponibles por los vendedores de estos equipos. Por ejemplo, Cisco ofrece amplia documentación en línea y libros impresos acerca de las características de seguridad de sus productos. Estos libros y documentos son valiosos, pero no son suficientes. La mayoría de los documentos suministrados por el proveedor de seguridad del router se centran en la documentación de todas las características de seguridad que ofrece el router, y no siempre ofrece un uso apropiado y racional de la seguridad que se puede configurar en el mismo.[24]

4.3 PRINCIPIOS DE SEGURIDAD EN ROUTERS Y OBJETIVOS

4.3.1 ¿Por qué un Router para fines específicos?: ¿Cuáles son algunas de las motivaciones para el uso de un Router, en lugar de una máquina de propósito general con un Sistema Operativo estándar? ¿Qué justifica este gasto, y lo que justifica la molestia de aprender otro sistema? La respuesta, en parte, concierne al rendimiento: Un Router para fines específicos puede tener un rendimiento mucho más alto que un ordenador de propósito general con funcionalidad de enrutamiento. Además, potencialmente se pueden añadir más conexiones de red a una máquina diseñada para este fin, puesto que puede estar diseñada para soportar más tarjetas de interfaz. Así, un dispositivo de propósito especifico, probablemente será una solución de menor costo para un determinado nivel de funcionalidad. Pero también hay una serie de prestaciones de seguridad en un router para fines específicos, en general, la consolidación de enrutamiento de la red y las funciones relacionadas a dispositivos dedicados restringen el acceso y los límites a la exposición de ciertas funciones críticas.

En primer lugar, un Sistema Operativo especializado, como el Cisco Internetwork Operating System (IOS) puede ser más pequeño, mejor comprendido y probado mas a fondo que un SO de propósito general. Esto significa que es potencialmente menos vulnerable. En segundo lugar, el mero hecho de que este Sistema Operativo sea diferente de los demás hace que un atacante tenga una cosa más que aprender, y que las vulnerabilidades conocidas en otros sistemas son de poca ayuda para el atacante del router. Por último, IOS permite una aplicación más completa y más robusta de filtrado. El filtrado es tan útil como un “firewall”, y también se puede particionar redes y prohibir o restringir el acceso a ciertas redes o servicios. El uso del filtrado le permite a los protocolos de

[24] Router Security Configuration Guide Principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

enrutamiento pueden publicar ciertas rutas seleccionadas hacia sus vecinos, contribuyendo así a proteger ciertas partes de su red.[25]

4.3.2 Ataques comunes en los routers: Las amenazas en general incluyen, pero no están limitados a: accesos no autorizados, robos de sesión, redireccionamiento, enmascaramiento, denegación de servicio (*DoS*)[26], espionaje (*eavesdropping*)[27], y robo de información. Además de las amenazas a un Router en la red, el acceso por Dial-up a un router lo expone a nuevas amenazas.

Las técnicas de ataque son: adivinar contraseñas, ataques a los protocolos de enrutamiento, ataques de SNMP, ataques de fragmentación de IP para eludir el filtrado, ataques de redireccionamiento, y redirección circular para denegación de servicio.

- Ataques de reproducción de sesión: Utilizan una secuencia de paquetes o comandos de aplicación que se pueden grabar, manipular, y luego repetir para provocar una acción o acceso no autorizado.
- Ataques de redireccionamiento: Pueden incluir la manipulación de las actualizaciones router para causar que el tráfico fluya a destinos no autorizados. Este tipo de ataques se denomina a veces "inyección de rutas".
- Ataques de enmascaramiento: Se producen cuando un atacante manipula los paquetes IP para falsificar direcciones IP. El enmascaramiento se puede utilizar para obtener acceso no autorizado o para inyectar datos falsos en una red.
- Robos de sesión: Se pueden producir si un atacante puede insertar paquetes IP falsos después de establecer una sesión a través de spoofing IP.
- Ataques de agotamiento de recursos: Generalmente implican inundar al router con tráfico o solicitudes diseñadas para consumir la totalidad de los recursos limitados de este. Estos recursos pueden ser: ancho de banda, memoria, o incluso la computación.

Una cuidadosa configuración del router puede ayudar a prevenir que la red sea atacada por un ataque (DDoS) Denegación Distribuida del Servicio, mediante el bloqueo de direcciones de origen falso. Los ataques DDoS utilizan un número de sitios para inundar a un sitio de

---

[25] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

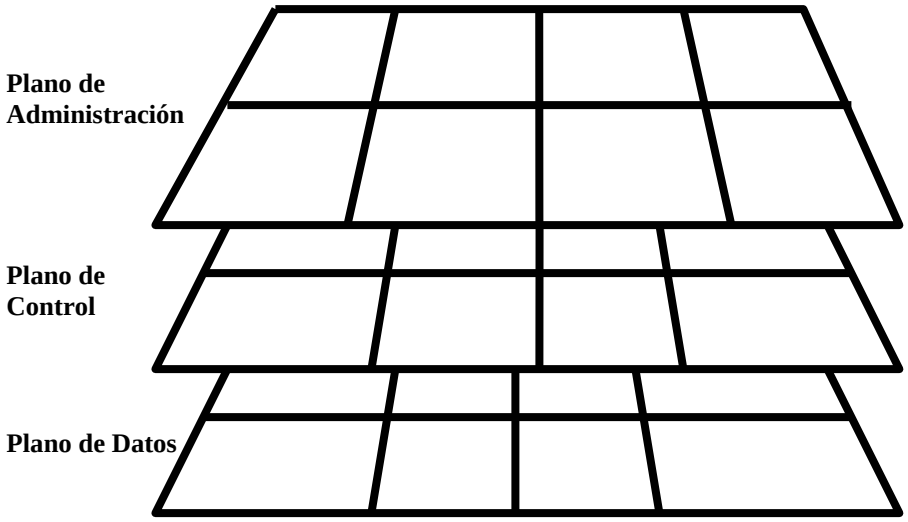
[26] DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

[27] Termino inglés que traducido al español significa escuchar secretamente, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad. http://es.wikipedia.org/wiki/Eavesdropping

destino con tráfico suficiente o con peticiones de servicio para que este quede inutilizable para los usuarios legítimos.[28]

4.3.3 Planos de operación de un router: Conceptualmente, un router opera en tres ámbitos o planos distintos. El plano Administrativo se encarga de la administración, configuración, y en general el estado del router. El plano de control comprende la supervisión, actualizaciones de la tabla de enrutamiento, y en general el funcionamiento dinámico del router. El plano de datos o el plano de reenvío se encarga de los paquetes que transitan por el router entre las redes a las que sirve.[29]

Figura 10. Planos de operación de un router



Fuente: Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

Para asegurar un router, debemos tener en cuenta las posibles amenazas en cada plano. Las amenazas al plano de Administración y al de control se refieren principalmente a los

[28] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

[29] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

accesos no autorizados al router, o a la interferencia con el funcionamiento del router. Las amenazas al plano de datos se refieren a violaciones de seguridad de red para las redes que apoya el router.[30]

4.4 SEGURIDAD DEL ROUTER

4.4.1 Seguridad Física: Hay un número de maneras para proporcionar seguridad física a un router. El centro de cómputo que contiene al Router debe estar libre de interferencias electrostáticas o magnéticas. Debería haber controles de temperatura y humedad. Si el funcionamiento continúo del router es fundamental, una fuente de alimentación ininterrumpida (UPS) debe ser instalada y componentes de repuesto tenerse a mano. Para ayudar a proteger al Router contra algunos ataques de denegación de servicio (DoS), y para que pueda apoyar la más amplia gama de servicios de seguridad, el router debe estar configurado con la máxima cantidad de memoria posible. Además, el router debe ser colocado en un cuarto cerrado sólo accesible al personal autorizado.

4.4.2 Sistema Operativo: El sistema operativo para el router es un componente crucial. Decidir qué características necesita la red, y utilizar la lista de características para seleccionar la versión del sistema operativo mas apropiada. Sin embargo, la última versión de cualquier sistema operativo no suele ser la más fiable debido a su limitada exposición en una amplia gama de entornos de red. Se debe utilizar la última versión estable del sistema operativo que cumpla con los requisitos y características de la red.

4.4.3 Fortalecer la configuración: Un router es similar a muchos equipos, ya que tiene muchos servicios activados por defecto. Muchos de estos servicios son innecesarios y pueden ser utilizados por un atacante para obtener información o para su explotación. Los servicios innecesarios deben ser desactivados en la configuración del router.

4.5 PROTEGIENDO LA RED CON EL ROUTER

4.5.1 Roles en la Seguridad y Operación de la Red: Los Routers realizan diferentes trabajos en las redes modernas, pero para esta discusión vamos a examinar tres aspectos fundamentales en las que se emplean los routers.

---

[30] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

4.5.1.1 Routers de Interior: Un Router interior reenvía el tráfico entre dos o más redes locales dentro de una organización o empresa. Las redes conectadas por un router de interior a menudo comparten la misma política de seguridad, y el nivel de confianza entre ellos es generalmente alto. Si una empresa tiene muchos routers internos, por lo general se empleara un Protocolo de Gateway Interior (IGP) para administrar El enrutamiento. Los Routers de Interior pueden imponer algunas restricciones en el tráfico que reenvían entre las redes.

4.5.1.2 Routers Backbone: Un Router Backbone o de Exterior es el que reenvía el tráfico entre las distintas empresas (a veces llamados "sistemas autónomos diferente"). El tráfico entre las distintas redes que conforman la Internet es dirigido por los Routers Backbone. El nivel de confianza entre las redes conectadas por un Router Backbone es generalmente muy bajo. Típicamente, los Routers Backbone se han diseñado y configurado para reenviar el tráfico lo más rápidamente posible, sin imponer ninguna restricción al respecto. Los objetivos principales de seguridad de los Routers de Backbone son para garantizar que la gestión y el funcionamiento de estos se realicen únicamente por partes autorizadas, y para proteger la integridad de la información de enrutamiento que se utiliza para reenviar el tráfico. Los Routers Backbone normalmente emplean Protocolos de Gateway Exterior (EGP) para administrar el enrutamiento. Configurar Routers Backbone es una tarea bastante especializada.

4.5.1.3 Routers de Borde: Un Router de Borde envía el tráfico entre una empresa y las redes exteriores. El aspecto clave de un Router de Borde es que representa la frontera entre las redes internas de confianza de una empresa, y las redes externas que no son de confianza (por ejemplo, Internet). Puede ayudar a asegurar el perímetro de una red empresarial mediante la aplicación de restricciones en el tráfico que maneja. Un Router de Borde utiliza protocolos de enrutamiento, o puede depender enteramente de rutas estáticas.

Típicamente, un Router de Borde no es el único componente en esa frontera, muchas empresas también utilizan un Firewall para que las políticas de seguridad se cumplan correctamente y se fortalezca aun mas.[31]

4.6 ASPECTOS DE LA SEGURIDAD DE LOS ROUTERS

4.6.1 Función de los Routers en la Seguridad de la Red: Una red básica se puede crear a partir de la interconexión de Switches Capa 2, y enrutar los paquetes IP capa 3 de esta red mediante el uso de un router.

---

[31] Router Security Configuration Guide Router Security Guidance Activity of the System and Network Attack Center (SNAC)

La seguridad de los routers, es un tema critico en la seguridad de la red, si un atacante obtiene acceso y compromete la seguridad de los routers, esto seria una gran ventaja para aumentar la vulnerabilidad de la red, conocer las funciones que cumplen los routers en la red, ayudara a comprender sus vulnerabilidades.

Los Routers cumplen las siguientes funcionalidades:

- Publicar las redes y filtrar a quienes pueden utilizarlas
- Proporcionar acceso a los segmentos de las redes y subredes

4.7 LOS ROUTERS SON OBJETIVOS PARA LOS ATAQUES A LA SEGURIDAD

Los routers son Gateways[32] que proporcionan acceso a otras redes, por lo tanto son objetivos obvios, propensos a una variedad de ataques.

4.7.1 Diversos problemas de Seguridad:

Comprometer el control de acceso a los Routers, puede dejar al descubierto la configuración de la red y por lo tanto permite la concreción de ataques a otros dispositivos de la red.

- Comprometer las tablas de enrutamiento, pueden disminuir el rendimiento de la red, denegar el servicio y exponer información confidencial.
- Configurar incorrectamente los filtros de acceso a la red, permite a los atacantes tener acceso a los componentes internos de la red para escaneos, lo que permite que los agresores no sean detectados.

Los agresores, pueden atacar los Routers de diversas formas, por lo que los Administradores de Red, no tienen un enfoque preciso para combatir estas agresiones, por lo que aquí se explorara la protección de los Routers y la buena practica de la Administración de la Seguridad.[33]

---

[32] Un Gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

[33] Router Security Configuration Guide. Router Security Guidance Activity of the System and Network Attack Center (SNAC)

4.8 HERRAMIENTAS PARA LA ADMINISTRACIÓN DE SEGURIDAD EN ROUTERS CISCO

Existen dos herramientas importantes que nos pueden ayudar a administrar y configurar la seguridad en nuestros routers Cisco.

Estas dos herramientas son:

- AutoSecure
- SDM (Cisco Security Device Manager)

AutoSecure más que una herramienta externa, es un conjunto de comandos que se pueden activar en los Routers Cisco. AutoSecure fue introducido en el IOS de Cisco en la versión 12.3(1).

4.8.1 Beneficios de AutoSecure

4.8.1.1 Configuración de Seguridad Simplificada: AutoSecure es un comando que ayuda a aquellos usuarios que no tienen una gran experiencia en el manejo de todas las propiedades del IOS de Cisco, a asegurar de forma sencilla los servicios que ofrece un Router.

4.8.1.2 Mejoramiento de Seguridad de Contraseñas: AutoSecure provee de los siguientes mecanismos para mejorar la seguridad de las contraseñas.

- La habilidad de configurar una longitud minima para las contraseñas, lo que contrarresta que se creen contraseñas fáciles de rastrear como “cisco” o “lab”.
- Mensajes de registro (Syslog mesages) son generados después de haber sobrepasado un numero de intentos fallidos.

4.8.1.3 Aseguramiento del Plano de Administración: Asegurar el plano de administración es uno de los objetivos de AutoSecure, el otro será descrito adelante y es el Aseguramiento del Plano de Datos. El Aseguramiento del plano de administración se realiza deshabilitando ciertos servicios e interfaces que pueden ser potencialmente explotados por los ataques a la seguridad y habilitando servicios globales para mitigar el intento de ataques a la seguridad.

AutoSecure asegura el plano administrativo de un router como sigue:

- Deshabilitar Servicios Globales
- Deshabilitar Servicios por Interfaz
- Habilitar Servicios Globales

4.8.1.4 Aseguramiento del Plano de Datos: Para minimizar los riesgos de ataque en el plano de datos del router. AutoSecure provee las siguientes funciones.

- Cisco Express Forwarding (CEF)[34] AutoSecure habilita CEF o CEF distribuido (dCEF) en el router cuando sea posible. Pues no es necesario construir entradas de cache cuando el trafico comienza a llegar a nuevos destinos
- Si el router esta siendo usado como Firewall, puede configurarse para (CBAC)[35] context-based access control en interfaces públicas que están de cara a Internet.

4.9 SDM (CISCO ROUTER AND SECURITY DEVICE MANAGER)

Cisco Security Device Manager es una herramienta basada en entorno Web embebida en el sistema operativo IOS de Cisco, SDM simplifica la configuración de la seguridad de los routers, a través de un conjunto de pantallas inteligentes, que le permiten al usuario final configurar e implementar la seguridad sin necesidad de tener conocimientos en el CLI de IOS.

4.9.1 Flexibilidad y Facilidad de Uso: SDM le permite al usuario configurar e implementar la seguridad de los routers Cisco y permite una administración interactiva. SDM permite implementar la configuración y monitoreo en un router nuevo o existente de forma remota, se pueden realizar estas operaciones sobre routers Cisco Seri 830, 1700, 2600xm, 3600 y 3700.

Esta aplicación esta diseñada tanto para expertos como para aquellos que no tienen un amplio conocimiento de la Línea de Interfaz de Comandos de IOS (CLI). Hemos terminado con los aspectos teóricos de la investigación, ahora pasaremos a la ingeniería del proyecto la cual nos mostrara como se prepara una red para implementar y configurar una VPN.

---

[34] CEF (Cisco Express Forwarding) es un feature avanzado de Cisco IOS que permita un modo de conmutación más rápido en los dispositivos Cisco

[35] Control de Acceso Basado en Contexto. Ofrece a los usuarios internos un control de acceso seguro por aplicación para todo el trafico a través de los parámetros, como por ejemplo perímetros en redes empresariales privadas e Internet

5. INGENIERIA DEL PROYECTO

5.1 PLANIFICACION DE LA CONFIGURACIÓN DE ROUTERS CISCO IOS PARA CLAVES PRECOMPARTIDAS SITIO A SITIO

En este capitulo se tratara la configuración de una VPN por medio del protocolo IPSec en Routers Cisco por medio del uso de claves precompartidas.
El proceso de configuración de las claves precompartidas del IKE del Software IOS de Cisco consta de cuatro tareas principales:

Tarea 1: Preparación para IPSec
Tarea 2: Configuración de IKE
Tarea 3: Configuración de IPSec
Tarea 4: Comprobación y Verificación de IPSec

Tarea 1: Determinación detallada de las normas de cifrado, identificación de los hosts y redes que desea proteger, determinación de los detalles sobre los iguales IPSec, Asegurarse de que las Listas de Control de Acceso (ACL) existentes sean compatibles con IPSec.

Tarea 2: Habilitar IKE, creando las normas IKE y validando su verificación.

Tarea 3: Definir los conjuntos de transformación, crear los mapas de cifrado y aplicarlo a las interfaces respectivas.

Tarea4: Utilizar los comandos básicos de comprobación de IOS de Cisco, tal como *show* y *debug.*

5.1.1 Preparación Para IPSec: Dependiendo del tamaño de la Red, la planificación para la implementación de este protocolo puede ser compleja, por tal motivo es importante que la preparación previa a la configuración de una VPN con IPSec debe ser lo mas detallada posible.

Si no se planifica con antelación y de forma correcta la configuración del cifrado IPSec, puede acarrear en errores de configuración que son difíciles de detectar una vez implementado el protocolo en la Red.

Las normas de seguridad de IPSec, deben estar basadas en las normas generales de seguridad de la empresa, por tal motivo, es necesario seguir unos pasos básicos para definir la configuración inicial y reducir al máximo los errores en el funcionamiento de la VPN:

- Fase uno de IKE (Determinación de la norma IKE). Determinar la norma IKE a usar entre los iguales de la red que van a estar involucrados en el funcionamiento de la VPN
- Fase dos de IKE (Determinación de la norma IPSec). Identificar los detalles del igual IPSec, Dirección IP, Conjuntos de transformación IPSec y modos IPSec, en este paso se configuran los mapas de cifrado.
- Comprobar la configuración actual. Utilizar los comandos básicos de comprobación como *show running-configuration*, *show isakmp policy* y *show crypto map* para verificar la configuración actual del Router al que se le aplicara IPSec.
- Asegurarse de que la Red funciona sin cifrado. Verificar que la red tenga la conectividad básica, en especial entre los iguales IPSec antes de configurar la VPN, por tal motivo se puede utilizar el comando ping para verificar este tipo de conexión.
- Asegurarse de que las ACL son compatibles con IPSec. Asegurarse que los routers de borde y las interfaces del router vecino permitan el trafico IPSec.

5.1.1.1 Fase uno de IKE: Determinar el método de distribución de clave: Basados en el numero y la localización de los iguales IPSec se puede distribuir la clave manualmente si es una red pequeña. Si es una red grande se pueden usar los Servidores CA.

Determinación del método de autenticación. Dependiendo del método de distribución de clave, se puede seleccionar el método de autenticación. IOS utiliza diversos métodos de autenticación como: Claves precompartidas y RSA.
Identificar direcciones IP y nombres de host.

Determinar los detalles a cada uno de los iguales IPSec que utilizaran ISAKMP y las claves precompartidas para establecer la Asociación de Seguridad, esta es la información que se usara para configurar IKE. Determinar las normas ISAKMP para los iguales. La norma ISAKMP define una combinación o suite, de parámetros de seguridad. La negociación ISAKMP comienza con que cada igual coincida con una norma común (compartida).

Detalles de la norma ISAKMP:

- Algoritmo de Cifrado.
- Algoritmo *hash.*
- Tiempo de vida de la AS de IKE.

El objetivo de esta etapa es planificar y reunir los datos precisos que se necesitaran en etapas posteriores y para minimizar los errores en la configuración.

Tabla 1. Parámetros Norma IKE

Parámetros Norma IKE						
Parámetro		**Valor Aceptado**		**Keyword**		**Por Defecto**
Algoritmo de Cifrado		DES 3DES AES		des 3des aes		Des
Algoritmo de Integración de Mensajes (hash)		SHA-1 MD5		sha md5		sha-1
Método de Autenticación		Claves precompartidas RSA Firmas RSA		pre-share rsa-encr rsa-sig		Firmas RSA
Parámetros de Intercambio de Claves		Diffie-Hellman 768 bits Diffie-Hellman 1024 bits		1 2		Diffie-Hellman 768 bits
Tiempo de Vida AS		Se puede especificar un numero en segundos				86400 Segundos

Fuente: Redes Privadas Virtuales de Cisco Secure. Planifique, desarrolle y mantenga redes privadas virtuales con el libro oficial CSVPN. Cisco Press. Capitulo 3 Configuración de routers Cisco IOS para claves precompartidas sitio-a-sitio.

5.1.1.2 Fase Dos De IKE: Seleccionar los algoritmos y parámetros IPSec para una seguridad y funcionamiento óptimos. Determina que tipo de seguridad IPSec utiliza al asegurar el tráfico de interés. Algunos de los algoritmos IPSec requieren un compromiso entre altas prestación y una seguridad más fuerte.

Selección de los conjuntos de transformación. Se utilizan los algoritmos IPSec anteriormente seleccionados para ayudar a seleccionar las transformaciones, conjuntos de transformación y modos de operación de IPSec.

Identificar los detalles IPSec del igual. Identificar la dirección IP y los nombres de host de todos los iguales IPSec con los que se conectara.

Determinar direcciones IP y aplicaciones host que se van a proteger. Decidir que aplicaciones host y direcciones IP se protegerán tanto en el router igual como en el remoto.

Seleccionar entre inicio manual o mediante IKE. Elegir si la AS se establecerá de forma manual o mediante IKE.

Tabla 2. Transformaciones IPSec para la Cabecera de autenticación

Cabecera de Autenticación (AH)			
ah-md5-hmac		Transformación AH-HMAC-MD5	
ah-sha-hmac		Transformación AH-HMAC-SHA	
ah-rfc1828		Transformación AH-MD (RFC1828) utilizada con las instalaciones IPSec mas antiguas	

Fuente: Redes Privadas Virtuales de Cisco Secure. Planifique, desarrolle y mantenga redes privadas virtuales con el libro oficial CSVPN. Cisco Press. Capitulo 3 Configuración de routers Cisco IOS para claves precompartidas sitio-a-sitio.

Tabla 3. Transformaciones IPSec para la Sobrecarga de Seguridad del Encapsulado

Sobrecarga de seguridad del encapsulado (ESP)			
esp-des		Transformación ESP con cifrado DES (56 bits)	
esp-aes		Transformación ESP con cifrado AES	
esp-3des		Transformación ESP con cifrado 3DES (168 bits)	
esp-md5-hmac		Transformación ESP con autenticación HMAC-MD5, utilizada con esp-des, esp-3des, esp-aes provee integridad adicional	
esp-sha-hmac		Transformación ESP con autenticación HMAC-SHA, utilizada con esp-des, esp-3des, esp-aes provee integridad adicional	
esp-null		Transformación ESP sin cifrado, no produce ninguna protección al	

		flujo de datos	
esp-rfc1829		Transformación ESP-DES-CBC (RFC1829) utilizada con las antiguas versiones de IPSec	

Fuente: Redes Privadas Virtuales de Cisco Secure. Planifique, desarrolle y mantenga redes privadas virtuales con el libro oficial CSVPN. Cisco Press. Capitulo 3 Configuración de routers Cisco IOS para claves precompartidas sitio-a-sitio.

5.1.1.3 Comprobación de la configuración actual: Se debe revisar la configuración actual de los routers par verificar si estos ya tienen una configuración IPSec preestablecida, por defecto los Routers Cisco tienen configurado ciertos parámetros para IPSec que se pueden y se deben usar, pero para evitar problemas y errores en la configuración, es mejor configurar una norma IKE e IPSec personalizada.

Para verificar si en el Router hay alguna configuración preestablecida, se puede usar el comando de configuración global *show running-configuration* o el comando *show crypto isakmp policy* para examinar la norma IKE preestablecida en la configuración por defecto del Router.

5.1.1.4 Asegurarse de que la Red funcione sin cifrado: Se debe verificar la configuración básica de los routers que van a participar en la creación de la VPN, el comando ping se puede utilizar para analizar la transmisión de paquetes por la red entre los dos Routers.

5.1.1.5 Asegurarse de que las Listas de Acceso son compatibles con IPSec: Hay que asegurarse de que las ACL configuradas en los Routers de borde, Firewalls PIX u otros dispositivos de borde permita el flujo de datos IPSec a través de la Red.

Normalmente estos dispositivos restringen el tráfico hacia la red por medio de las Listas de Control de Acceso, por tal motivo, se debe verificar que los Datos ISAKMP, cabecera de autenticación (AH) y sobrecarga de seguridad del encapsulado (ESP) estén permitidos, ISAKMP utiliza el puerto 500 UDP, AH el puerto IP 51 y ESP el puerto IP 50.

Para verificar las ACL en el Router se debe utilizar el comando de configuración global *show access-lists.*

5.1.2 Configuración de IKE: Con los pasos y las configuraciones anteriormente mencionadas, se facilita la configuración de IKE en los Routers Cisco.

La configuración de IKE requiere de estos pasos y comandos esenciales:

- Habilitar o Deshabilitar IKE por medio del comando crypto isakmp enable. Este comando habilita el comando de configuración para configurar IKE en un Router Cisco. IKE por defecto ya esta habilitado en los routers Cisco, se puede utilizar el comando *no crypto isakmp enable* para deshabilitar esta función.
- Crear la norma IKE con los comandos *crypto isakmp policy*. En este paso se comienzan a definir las normas ISAKMP en los routers, se crea una sesión entre iguales ISAKMP. Se deben utilizar los detalles IKE recopilados en la Tarea 1 para configurar esta parte del proceso. El comando de configuración que se utiliza para habilitar la norma IKE es *crypto isakmp policy* [prioridad]. Prioridad identifica la norma IKE y le asigna una prioridad se utilizan valores entre 1 a 10000, siendo 1 la mas alta y 10000 la mas baja.
- Configuración de la Clave precompartidas con el comando *crypto isakmp key* y sus comandos asociados. Los iguales ISKMP se autentican mediante el uso de Claves precompartidas y la identidad ISAKMP, la identidad puede ser la dirección IP del router o el nombre de host, por norma la identidad ISAKMP se habilita por medio de la dirección IP, si se habilita la identidad por el nombre de host seria necesario utilizar un DNS dentro de la red, o habilitar la función DNS en el Router.
- Verificar la configuración de IKE. Se utilizan los comandos de configuración global *show crypto isakmp policy* para verificar la norma configurada.

Tabla 4. Palabras clave del modo de configuración *config-isakmp*

Palabras clave en el modo de configuración config-isakmp						
Palabra Clave		**Valores aceptados**		**Valores predeterminados**		**Descripción**
des		DES-CBC de 56 bits		des		Algoritmo de cifrado del mensaje
sha		SHA-1 (variante HMAC)		sha		Algoritmo de integridad de mensajes (hash)
md5		MD5 (variante HMAC)		sha		Valores aceptados
rsa-sig		Firmas RSA		rsa-sig		Método de autenticación del igual
rsa-encr		Números Aleatorios Cifrados				Método de autenticación del igual
pre-share		Claves precompartidas				Método de autenticación del igual
1		Diffie-Hellman		1		Parámetros

		768 bits				de intercambio de clave
2		Diffie-Hellman 1024 bits		2		Parámetros de intercambio de clave
Lifetime		Puede especificar cualquier tiempo en segundos		86400 segundo		Tiempo de vida de la AS establecida
Exit						Salida del modo config-isakmp

Fuente: Redes Privadas Virtuales de Cisco Secure. Planifique, desarrolle y mantenga redes privadas virtuales con el libro oficial CSVPN. Cisco Press. Capitulo 3 Configuración de routers Cisco IOS para claves precompartidas sitio-a-sitio.

5.1.3 Configuración de IPSec: Esta tarea consiste en configurar los datos anteriormente recopilados para IPSec en la Tarea 1 y se rige por los siguientes pasos:

- Configurar las suites de conjuntos de transformación con el comando *crypto ipsec transform-set.*
- Configurar los tiempos de vida globales de las asociaciones de seguridad de IPSec con el comando *crypto ipsec security-association lifetime.*
- Configurar las ACL de cifrado con el comando *access-list.*
- Configurar los mapas de cifrado con el comando *crypto map.*
- Aplicar los mapas de cifrado a las interfaces de destino o de origen.

5.1.3.1 Configurar las suites de conjuntos de transformación con el comando *crypto ipsec transform-set.:* Un conjunto de transformación es una combinación de transformaciones IPSec para ratificar una norma de seguridad especificada para el tráfico.

Los conjuntos de transformación combinan los siguientes factores IPSec:

- Mecanismo para autenticar la cabecera de autenticación: Transformación AH.
- Mecanismo para cifrar la sobrecarga: Transformación ESP
- Modo IPSec: Modo túnel o Modo Transporte.

Por defecto no se configura un conjunto de transformación para la Cabecera de autenticación AH, debido a que ESP provee encriptación y autenticación, mientras que AH solo provee autenticación.

Ejemplo: crypto ipsec transform-set prueba esp-md5-hmac esp-des

En el ejemplo anterior se configura un conjunto de transformación IPSec de nombre prueba que tiene por autenticación esp-md5-hmac y por cifrado esp-des.

5.1.3.2 Configuración de los tiempos de vida globales de las AS de IPSec con el comando *crypto ipsec security-association lifetime.*: El tiempo de vida de la AS, determina en cuanto tiempo las AS son validas y se ejecutan, una vez terminado este tiempo de vida, las asociaciones de seguridad se negocian y se vuelve a iniciar el tiempo de vida.

Ejemplo: crypto ipsec security-association lifetime 200 seconds

En el anterior ejemplo se configura un tiempo de vida para la AS de 200 segundos, tiempo en el que la VPN se establece, y pasado este tiempo la VPN se renegocia y las asociaciones de seguridad se vuelven a establecer.

5.1.3.3 Configurar las ACL de cifrado con el comando *access-list.*: Estas Listas de Control de Acceso de cifrado, se configuran para definir que trafico es el que se va a permitir a través de la VPN y que hosts o redes se van a comunicar a través de la VPN.

Ejemplo: access-list 101 permit ip 192.168.10.1 0.0.0.255 192.168.10.5 0.0.0.255

Este Ejemplo nos muestra una lista de acceso identificada con el número 101 que permite la comunicación ip entre la red 192.168.10.1 y la red 192.168.10.5.

5.1.3.4 Configurar los mapas de cifrado con el comando *crypto map.*: Se configuran los mapas de cifrado con el fin de configurar las AS para los flujos de datos que se deben cifrar.

Estas configuran los parámetros AS:

- Trafico de debe protegerse mediante IPSec (ACL de cifrado).
- Granularidad del tráfico a proteger por un conjunto de AS.
- Donde se debe enviar el trafico cifrado (Igual IPSec).
- Dirección local que se debe utilizar para el trafico IPSec.
- El tipo de seguridad IPSec que debe aplicarse al tráfico (conjuntos de transformación).
- Si las AS se establecen manual o a través de IKE.

Un mapa de cifrado se puede asignar solo una vez a una interfaz.

Ejemplo: crypto map VPN 10 ipsec-isakmp.

Este ejemplo muestra la configuración mas común de un mapa de cifrado para configurar una VPN, el nombre VPN es el nombre con el que se va a llamar al mapa de cifrado, y el numero 10 representa la entrada del mapa de cifrado, este numero es un identificador para este mapa de cifrado, si se crean mas mapas de cifrado para otras interfaces, se les asignan distintos números de identificación.
La sentencia ipsec-isakmp indica que este mapa es un mapa que va a establecer una asociación de seguridad por medio de IKE.
5.1.3.5 Aplicar los mapas de cifrado a las interfaces de destino o de origen.: El ultimo paso en la configuración de IPSec es asignar el mapa de cifrado anteriormente creado a la interfaz correspondiente, normalmente el mapa de cifrado se configura a la interfaz de salida del router que lleva el trafico hacia Internet.

Ejemplo: Router (config-if)# interface serial s0/0/0
Router (config-if)# crypto map VPN

En este Ejemplo se muestra el ingreso a la interfaz serial de un Router a la cual por medio del comando crypto map VPN se le esta asignando el mapa de cifrado que se configuro anteriormente.

5.1.4 Comprobación y verificación de IPSec: La última tarea para configurar una VPN por medio de IPSec es realizar la verificación y la comprobación del correcto funcionamiento de esta, para esto se utilizan varios comandos de configuración global en el router como el comando *show* y *debug.*

Utilizando ciertos comandos, se puede verificar las siguientes configuraciones y su correcto funcionamiento:

- Mostrar las normas IKE utilizando el comando *show crypto isakmp policy*
- Mostrar los conjuntos de transformación configurados utilizando el comando *show crypto ipsec transform-set.*
- Mostrar el estado actual de la AS con el comando *show crypto ipsec sa*
- Consultar los mapas de cifrado configurados con el comando *show crypto map*
- Depurar el trafico IKE e IPSec con los comandos *debug crypto ipsec* y *debug crypto isakmp*

6. DISEÑO INGENIERIL

6.1 IMPLEMENTACION INGENIERIL

6.2 CASO DE ESTUDIO DESARROLLO DE UNA VPN DE SITIO A SITIO CON EL PROTOCOLO IPSEC EN ROUTERS CISCO.

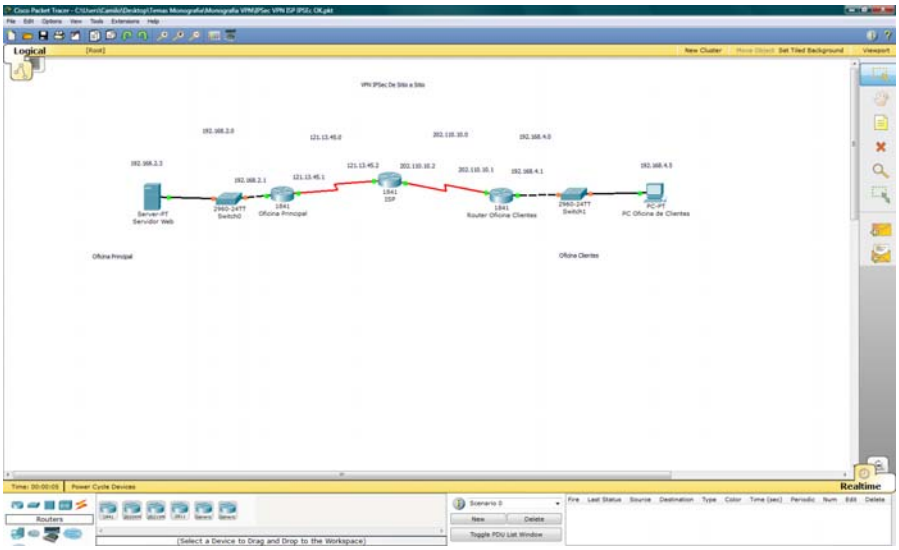
Se diseño un caso de estudio en Packet Tracer 5.2 el cual expone con detalle la configuración correcta y detallada de una VPN con IPSec de sitio a sitio, es decir de Router a Router.

6.3 CASO DE ESTUDIO VPN DE SITIO A SITIO

Una pequeña compañía ha establecido conectividad a Internet con dos Routers clase 1841, uno esta ubicado en su sede central, y el otro esta ubicado en una sucursal, les gustaría accesar a servicios entre los sitios, pero les preocupa que el tráfico de Internet no sea seguro. Para atender esta preocupación, se les ha sugerido que implementen una VPN de sitio a sitio. Una VPN permitiría que el sitio de la sucursal se conectara al sitio central de forma segura creando un túnel VPN que encriptaria y descifraría los datos.

Con respecto a la Topología se usara el Software IOS De Cisco de ambos Routers clase 1841 para configurar los parámetros de la VPN, la VPN se llamara VPN con autenticación SHA-1, encriptación AES y una Clave precompartida llamada VPNp31nc1paL.

Figura 11. Pantallazo General Caso Estudio Packet Tracer

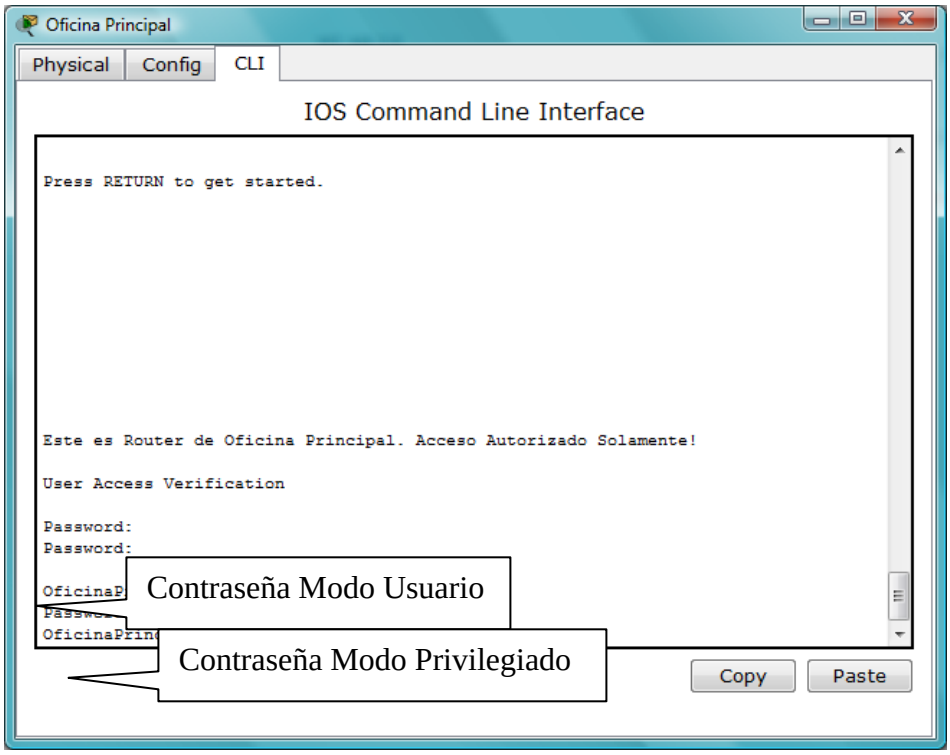


Fuente: Cisco Packet Tracer Versión 5.2

El software utilizado por los Routers Cisco 1841 es el IOS software versión 12.4 (15) T1.

El Router de la Oficina principal esta configurado para que solo el administrador de la red pueda accesar a el, el router esta configurado con sistema de contraseña tanto para modo Exec Usuario como para modo Exec Privilegiado.

Figura 12. Router Oficina Principal – Validación de Contraseñas



Fuente: Cisco Packet Tracer Versión 5.2

Para realizar la configuración de la VPN, es necesario seguir las 4 tareas de cifrado IPSec.

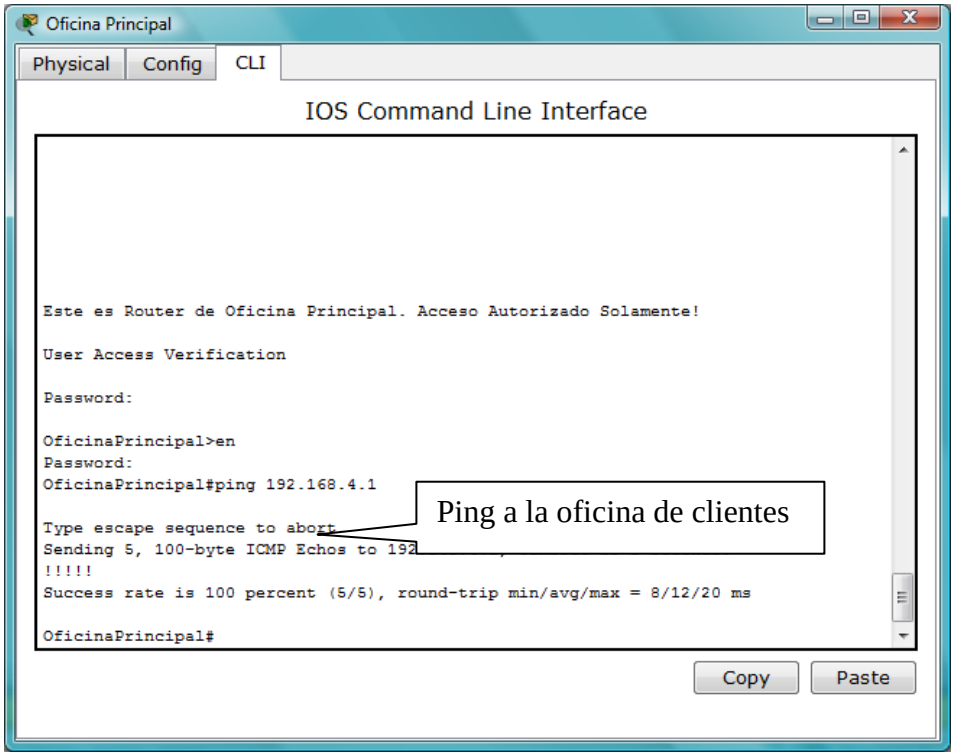
1. Preparación para IPSec
2. Configuración de IKE
3. Configuración de IPSec
4. Comprobación y verificación de IPSec[36]

Preparación para IPSec: La red del Caso de Estudio consta de una oficina principal y una sucursal u oficina de clientes que se encuentran conectadas entre ellas por un ISP, el cual les da acceso a la información de la red a través de Internet.

[36] Planificación de la configuración de routers cisco IOS para claves precompartidas sitio a sitio

El direccionamiento de la red de la Oficina Principal es 192.168.2.0 y el direccionamiento de la red de la Oficina de Clientes es 192.168.4.0, ambos direccionamientos, son direccionamientos privados necesitan transmitir su información a través de Internet.
Verificamos que la transmisión de datos se realiza perfectamente sin las VPN, al realizar una prueba de ping del Router de la Oficina Principal al Router de la Oficina de Clientes.[37]

Figura 13. Ping del Router Principal a la Oficina Clientes

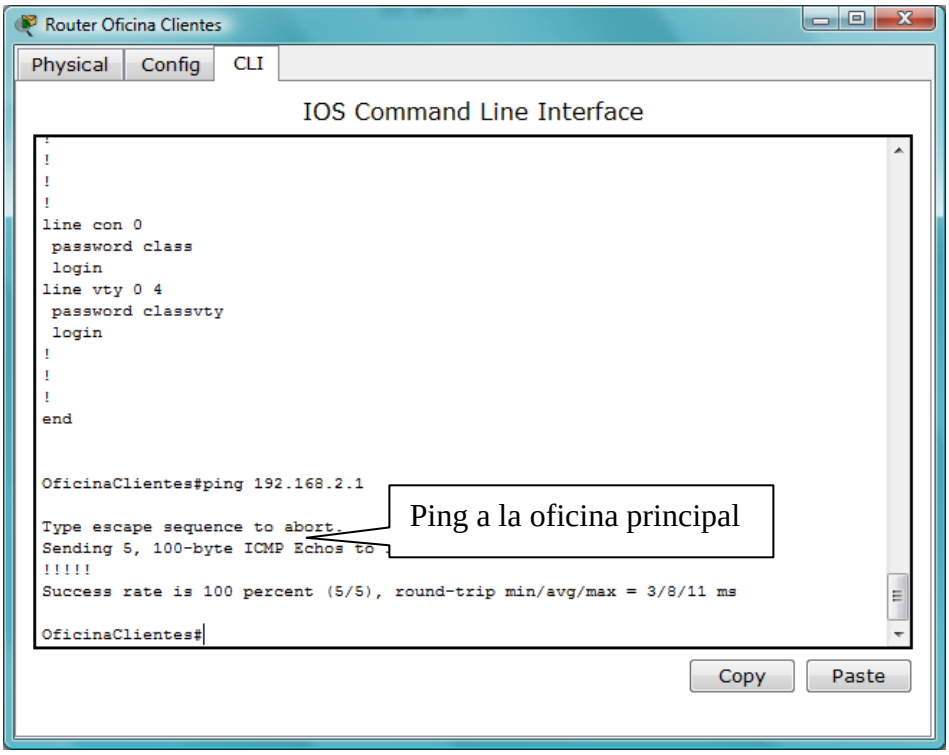


Fuente: Cisco Packet Tracer Versión 5.2

De la misma forma verificamos que la transmisión de datos se realiza de forma correcta desde la oficina clientes a la oficina principal.

[37] Ingeniería del Proyecto. 5.1.1 Preparación para IPSec. Asegurarse de que la Red funciona sin cifrado

Figura 14. Ping Router Clientes a Oficina Principal

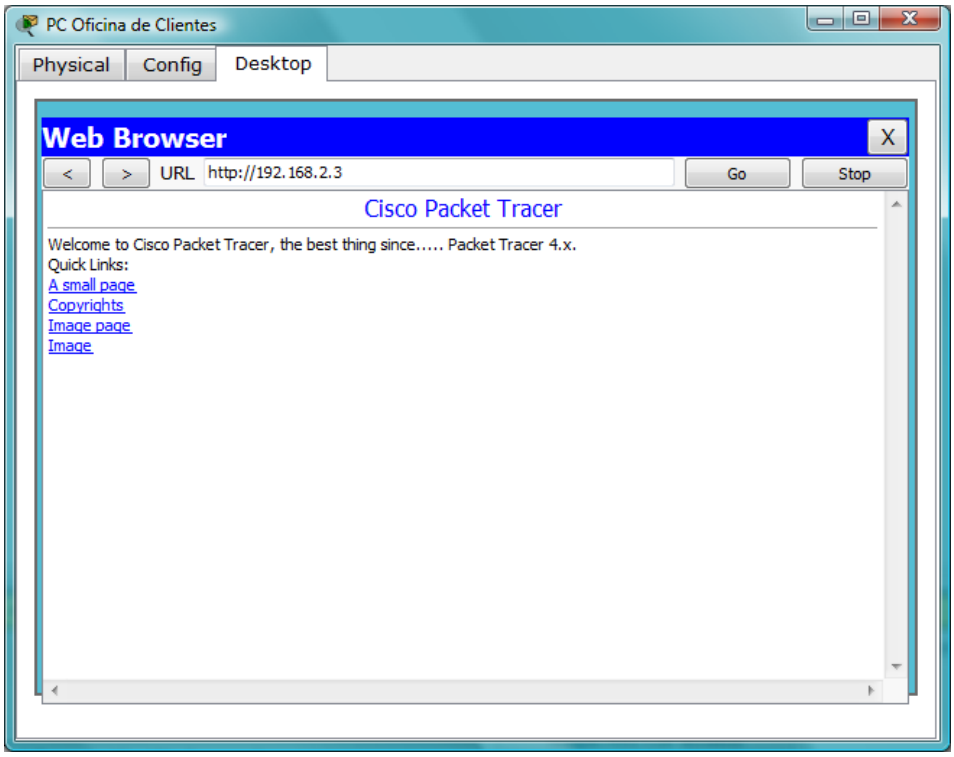


Fuente: Cisco Packet Tracer Versión 5.2

La transmisión de datos, como por ejemplo, acceder a una página Web del servidor desde la Computadora de la oficina de clientes se realiza sin ningún problema.[38]

[38] Ingeniería del Proyecto. 5.1.1 Preparación para IPSec. 5.1.1.4 Asegurarse de que la Red funciona sin cifrado

Figura 15. Acceso a la página Web del Servidor desde la PC Oficina Clientes



Fuente: Cisco Packet Tracer Versión 5.2

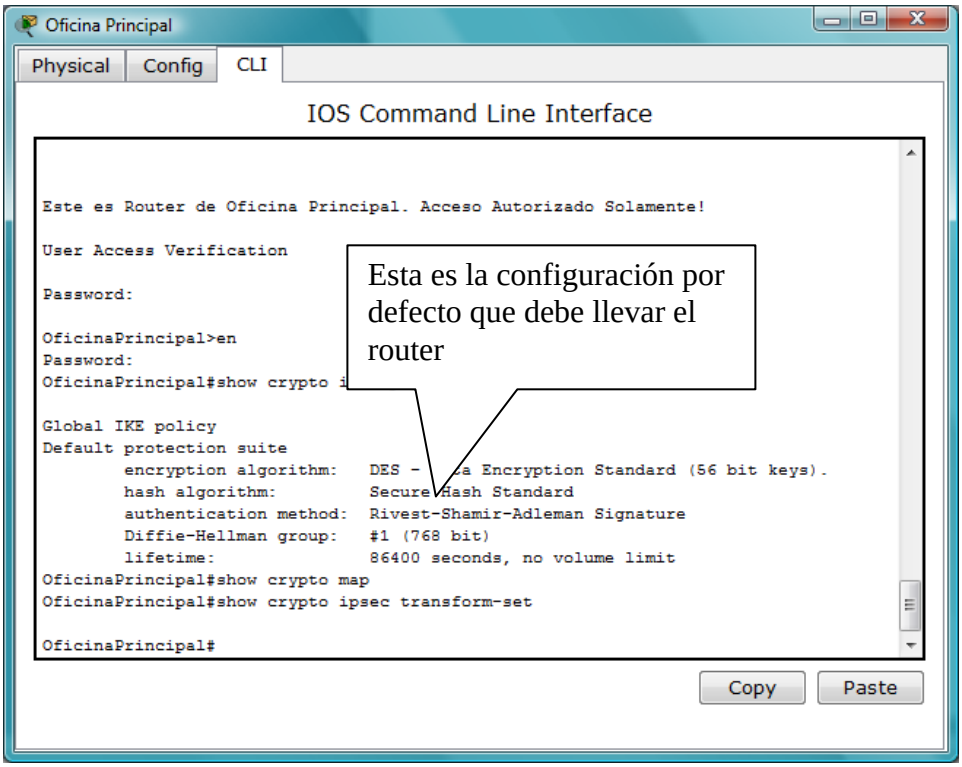
Al configurar la VPN entre los dos routers estamos creando un túnel entre ambos lo que nos provee de encapsulamiento y encriptación de los datos, y esto hace que la comunicación sea más segura entre los dos extremos.

Debido a que nuestra red, no tiene ningún tipo de configuración de VPNs nos aseguramos de que la configuración actual de los dos routers no haya tenido ninguna modificación.

Para revisar si hay alguna norma IPSec anteriormente configurada utilizamos el comando *show crypto isakmp policy* para examinar las normas IKE, el comando *show crypto map* para verificar si existe algún mapa de cifrado y el comando *show crypto ipsec transform-set* para verificar si existe algún conjunto de transformación previamente configurado.[39]

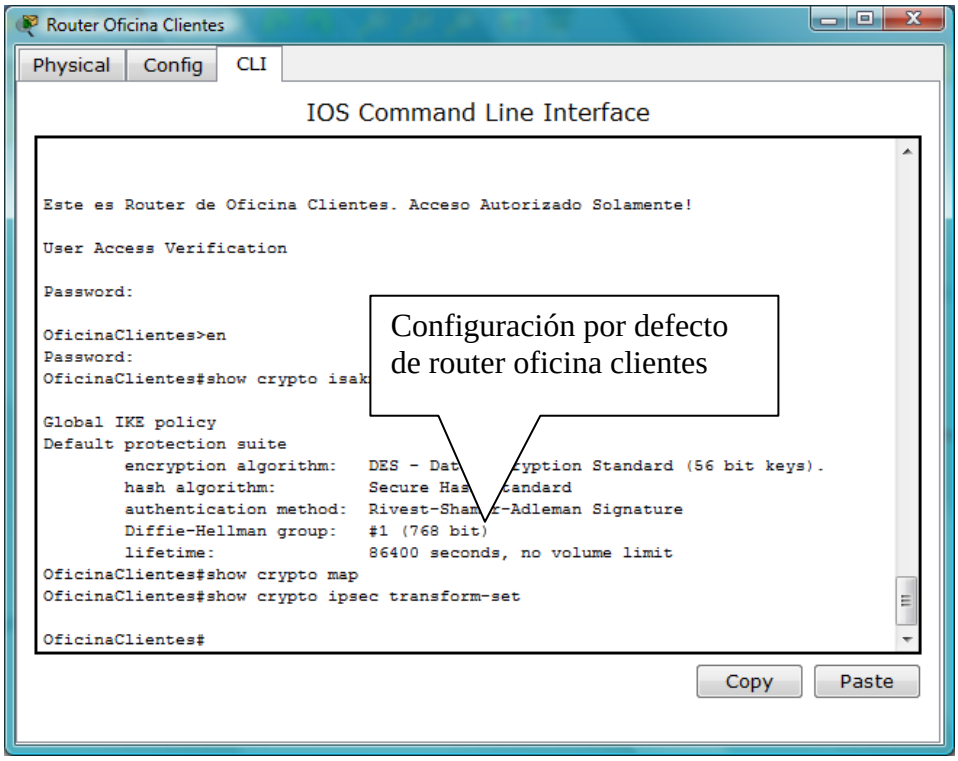
[39] Ingeniería del Proyecto. 5.1.1 Preparación para IPSec. 5.1.1.3 Comprobación de la Configuración actual

Figura 16. Configuración por Defecto del Router



Fuente: Cisco Packet Tracer Versión 5.2

Figura 17. Comprobación configuración actual Oficina Principal

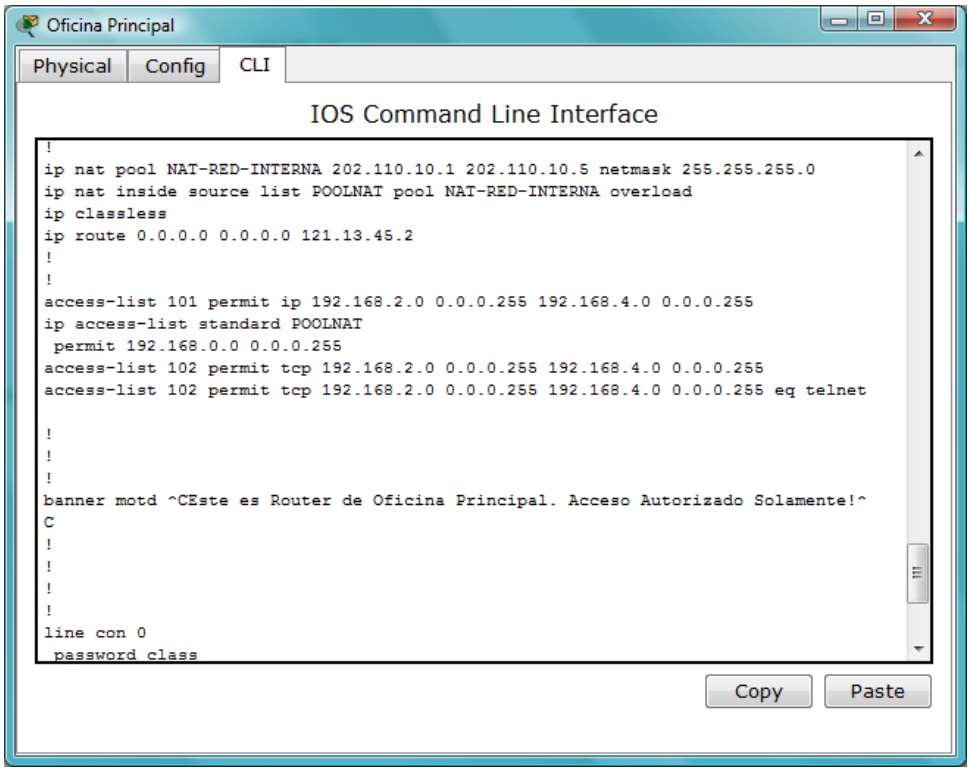


Fuente: Cisco Packet Tracer Versión 5.2

Debido a que ambas redes se encuentran en un lugar geográfico apartado, y aunque su direccionamiento IP es similar, para que el ISP pueda conectar a través de Internet a estas dos redes, se han creado una Listas de Acceso, para que estas dos redes se puedan conectar a través de una red publica, recordemos que las redes tienen direccionamiento IP privado, y para hacer la conexión con el ISP es necesario crear una Lista de Acceso que me conecte ambas redes a través de un direccionamiento publico.[40]

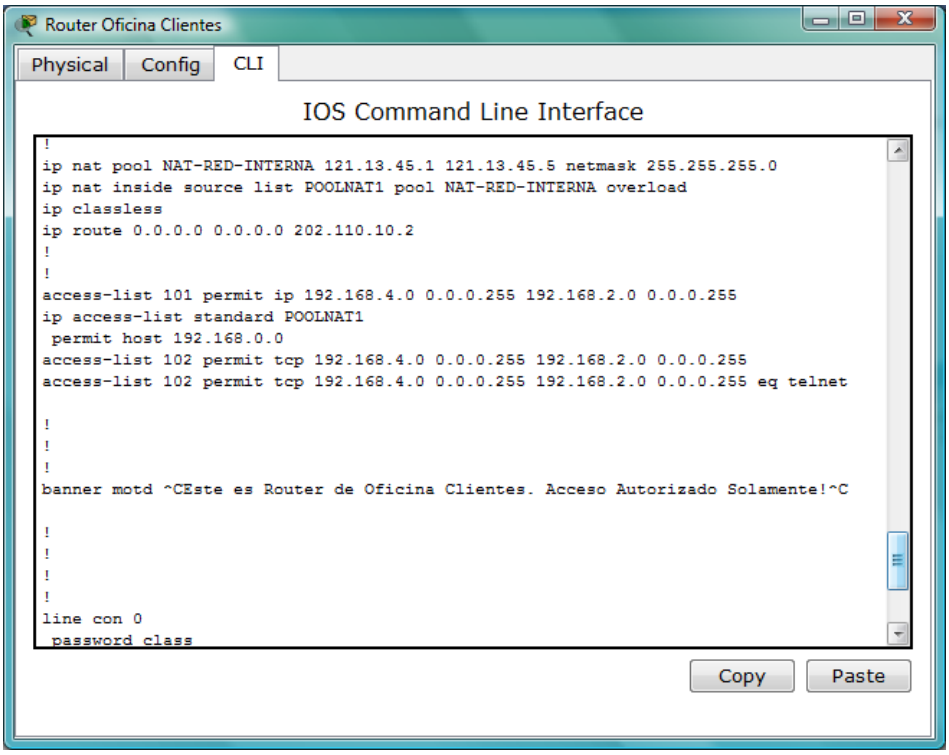
[40] Ingeniería del Proyecto. 5.1.1 Preparación para IPSec. 5.1.1.5 Asegurarse de que las ACL son compatibles con IPSec

Figura 18. Listas de Acceso para router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

Figura 19. Listas de Acceso para router oficina clientes



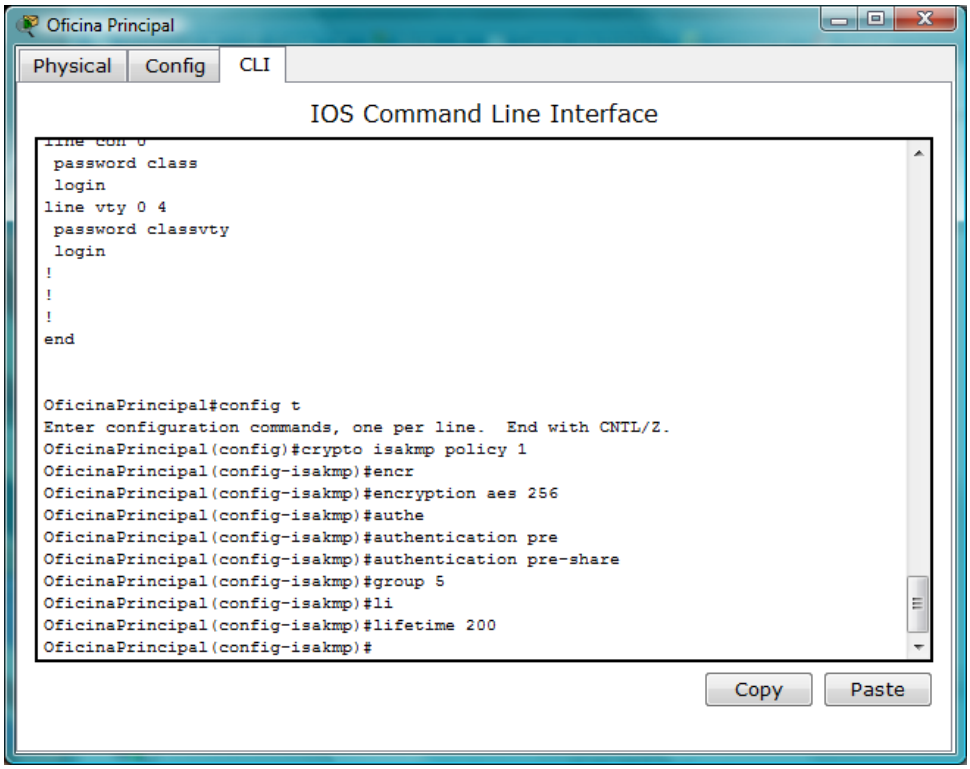
Fuente: Cisco Packet Tracer Versión 5.2

Configuración de IKE: Una vez hemos revisado que las listas de acceso permiten la correcta conexión entre las dos redes, procedemos a crear la norma IKE para cada uno de estos routers

El objetivo de esta configuración, es crear una sesión entre iguales ISAKMP entre dos extremos IPSec, por lo tanto usamos el comando *crypto isakmp policy*.[41]

[41] Ingeniería del Proyecto. 5.1.2 Configuración de IKE. Crear la norma IKE con los comandos crypto isakmp policy

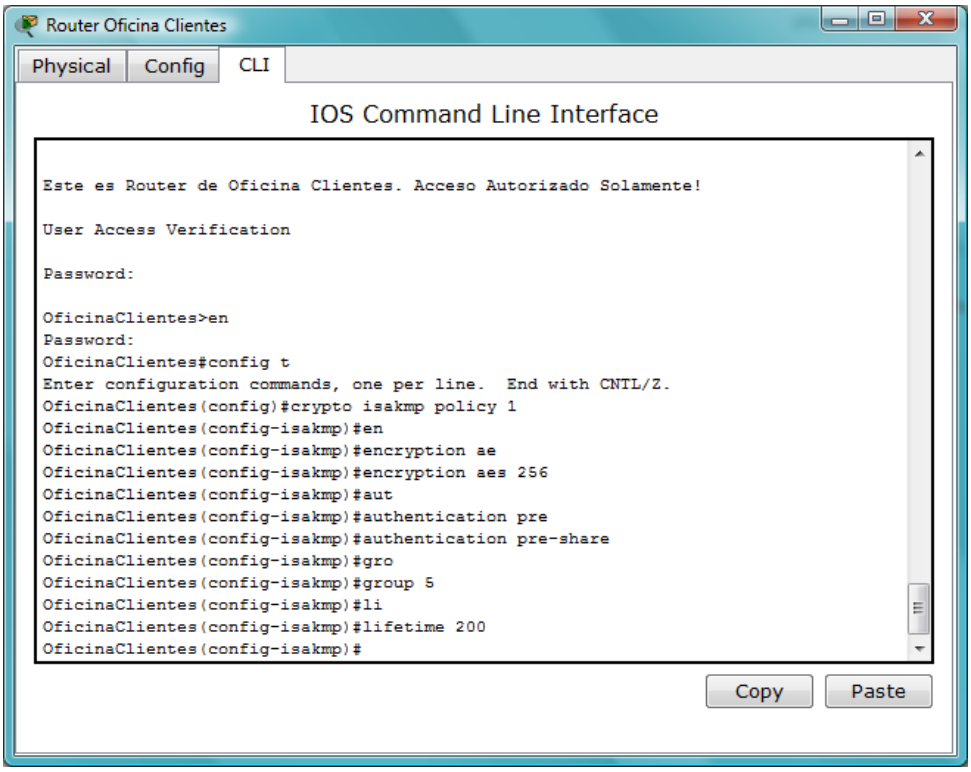
Figura 20. Creación de la norma IKE para router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

Como lo describe la figura arriba, hemos creado una norma IKE con prioridad 1, con un algoritmo de cifrado de mensajes tipo aes de 256 bits, autenticación de claves precompartidas, identificador de grupo Diffie-Hellman nivel 5 (Se ha escogido un nivel 5 de Diffie-Hellman, pues este contiene 1536 bits y provee mayor seguridad que un nivel 1 o 2) y un tiempo de vida de la asociación de seguridad de 200 segundos.

Figura 21. Creación de la norma IKE para router oficina clientes



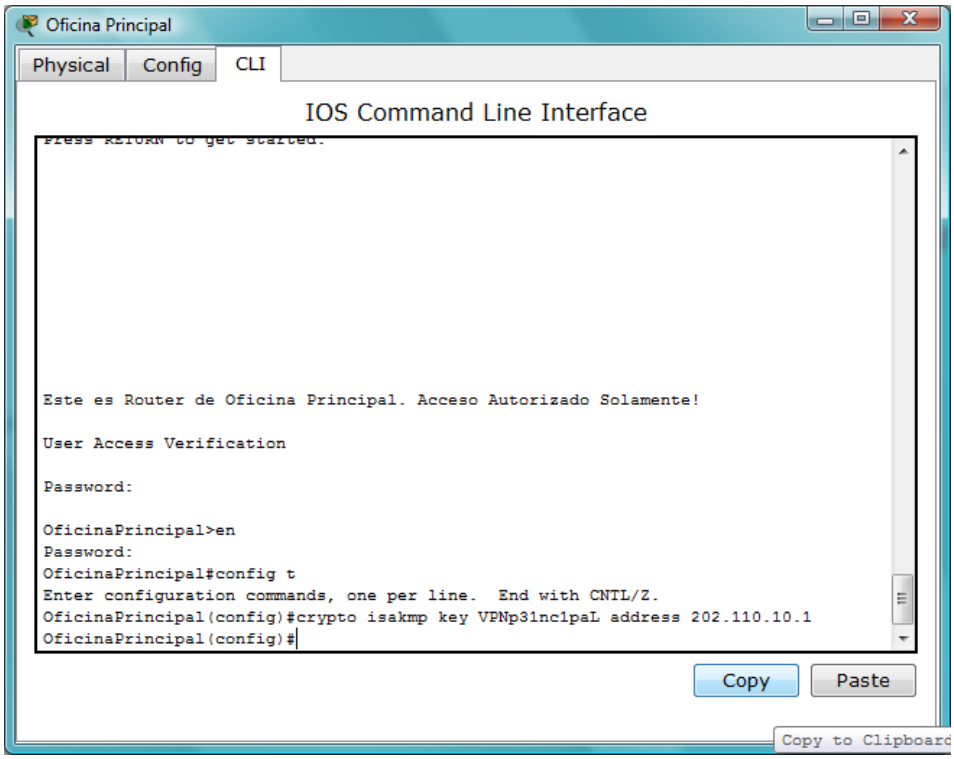
Fuente: Cisco Packet Tracer Versión 5.2

El mismo proceso se realiza en el router de la oficina clientes.

El siguiente paso a realizar es establecer las claves precompartidas, esto hace que los iguales IPSec se autentican el uno al otro durante las negociaciones ISAKMP utilizando la clave precompartida y la identidad ISAKMP (norma IKE).[42]

[42] Ingeniería del Proyecto. 5.1.2 Configuración de IKE. Configuración de la clave precompartida con el comando crypto isakmp key y sus comandos asociados

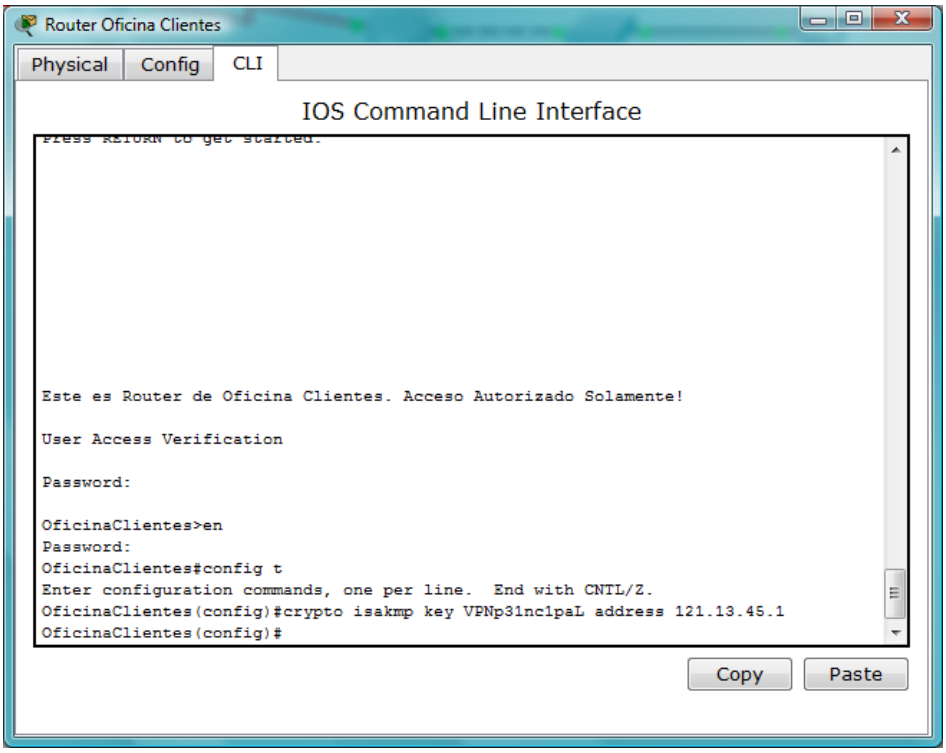
Figura 22. Creación clave precompartida router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

En el router de la oficina principal, hemos configurado una clave precompartida VPNp31nc1paL y que se debe validar en la dirección IP 202.110.10.1 esta dirección es la dirección IP del router de la oficina clientes.

Figura 23. Creación clave precompartida router oficina clientes



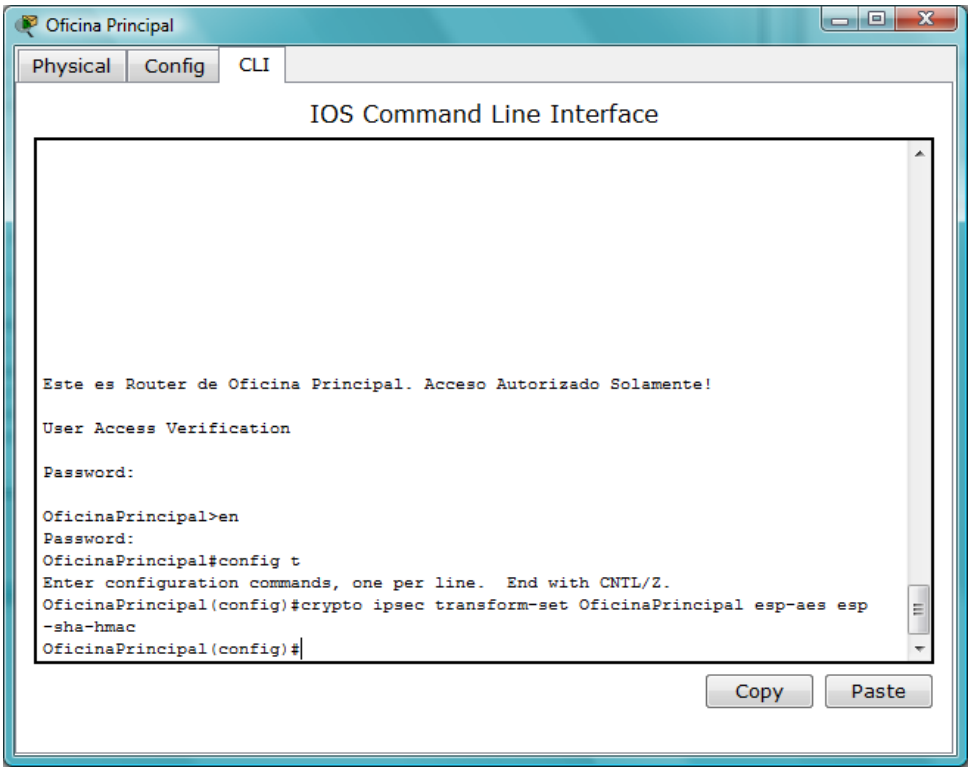
Fuente: Cisco Packet Tracer Versión 5.2

El mismo proceso se realiza en el router de la oficina clientes, se crea una clave precompartida VPNp31nc1paL y que se valide en la dirección IP 121.13.45.1 que es la dirección IP del router de la oficina principal.

Configuración de IPSec: La siguiente tarea es la configuración de IPSec en ambos iguales, comenzando con la configuración de las suites de conjuntos de transformación, estos conjuntos de transformación son los encargados de invocar la transformación cifrada, es decir como se autenticaran y se cifraran los paquetes dentro del túnel de la VPN.[43]

[43] Ingeniería del Proyecto. 5.1.3 Configuración de IPSec. 5.1.3.1 Configurar las suites de conjuntos de transformación con el comando crypto ipsec transform-set

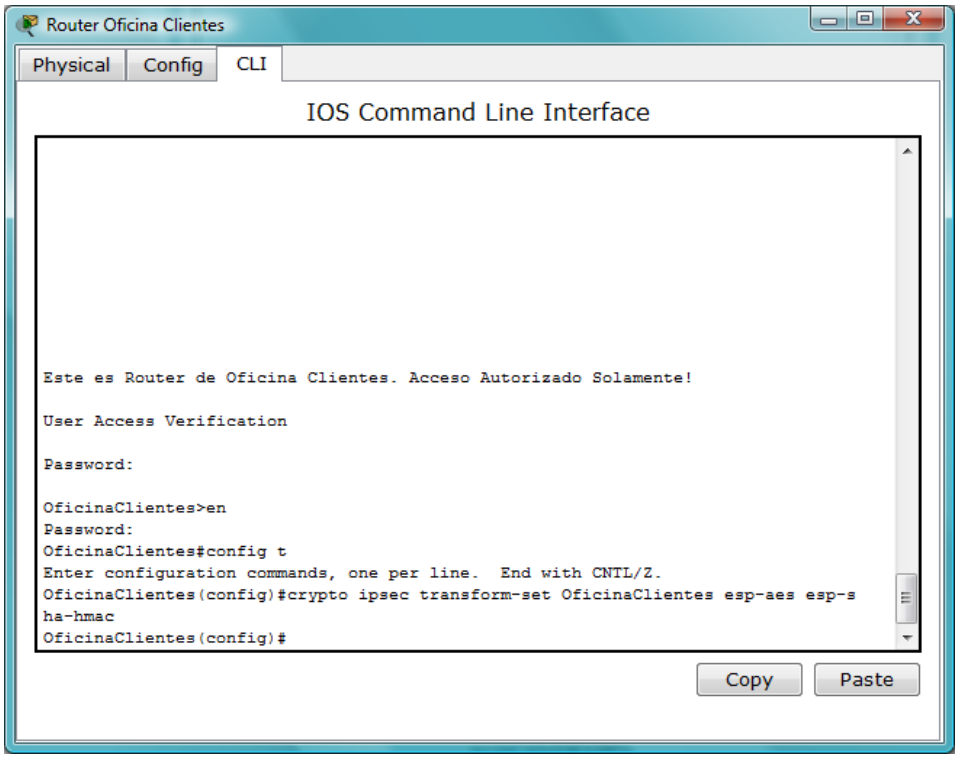
Figura 24. Creación del conjunto de transformación de router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

Se le debe dar un nombre al conjunto de transformación, en este caso, se le ha llamado OficinaPrincipal, pues esta siendo configurado en este router, el comando *crypto ipsec transform-set OficinaPrincipal esp-aes esp-sha-hmac* tiene dos partes fundamentales: la parte donde especifica la autenticación de los paquetes que es: *esp-aes* y el cifrado *esp-sha-hmac*.

Figura 25. Creación del conjunto de transformación de router oficina clientes



Fuente: Cisco Packet Tracer Versión 5.2

El mismo proceso se realiza en el router de la oficina de clientes, nombrando al conjunto de transformación OficinaClientes y configurando la autenticación y el cifrado de la misma forma como se hizo en el router de la oficina principal.

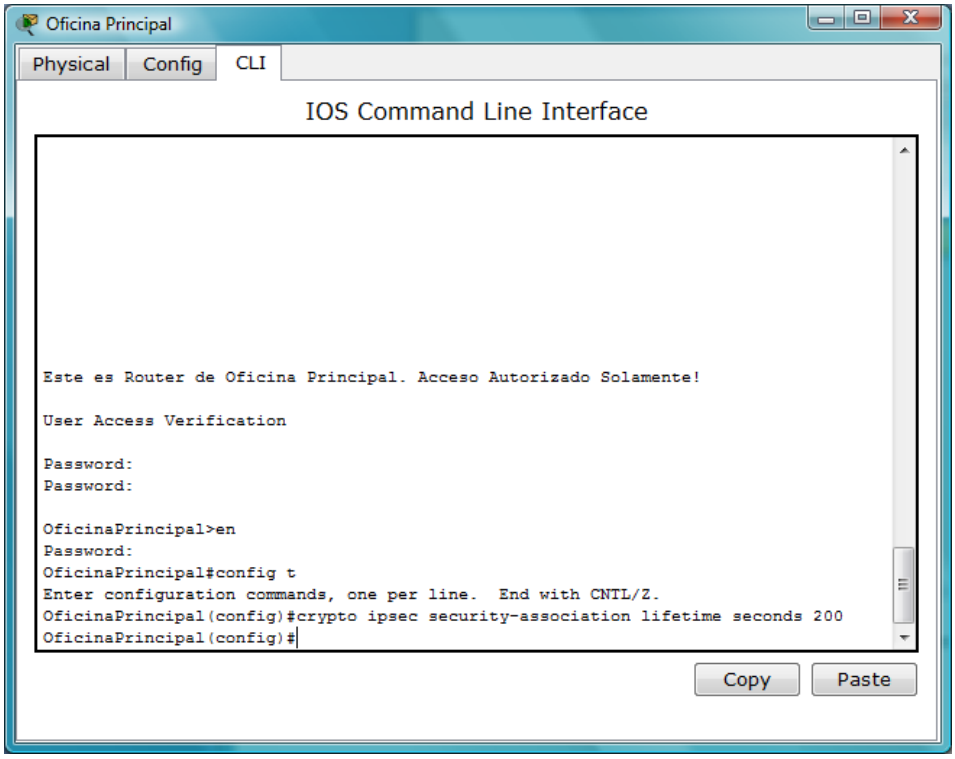
El siguiente paso, una vez configurados los conjuntos de transformación en ambos routers, es configurar los tiempos de vida globales de las Asociaciones de Seguridad (AS) de IPSec.

Estos tiempos de vida determinan cuanto tiempo son validas las AS entre los iguales (Routers) es decir, en estos tiempos de vida se crea el túnel entre los routers, se generan los conjuntos de transformación, con sus respectivas autenticaciones y cifrados.

Una vez el tiempo de vida expira, el túnel ya no está disponible, por lo que se realiza una reconexión automática del túnel.

Es recomendable siempre utilizar tiempos de vida cortos, pues al dejar tiempos de vida tan largos se corre el riesgo de que usuarios externos que deseen atacar a la VPN puedan tener más probabilidades de éxito de vulnerar la seguridad.[44]

Figura 26. Configuración del tiempo de vida de la AS de router oficina principal

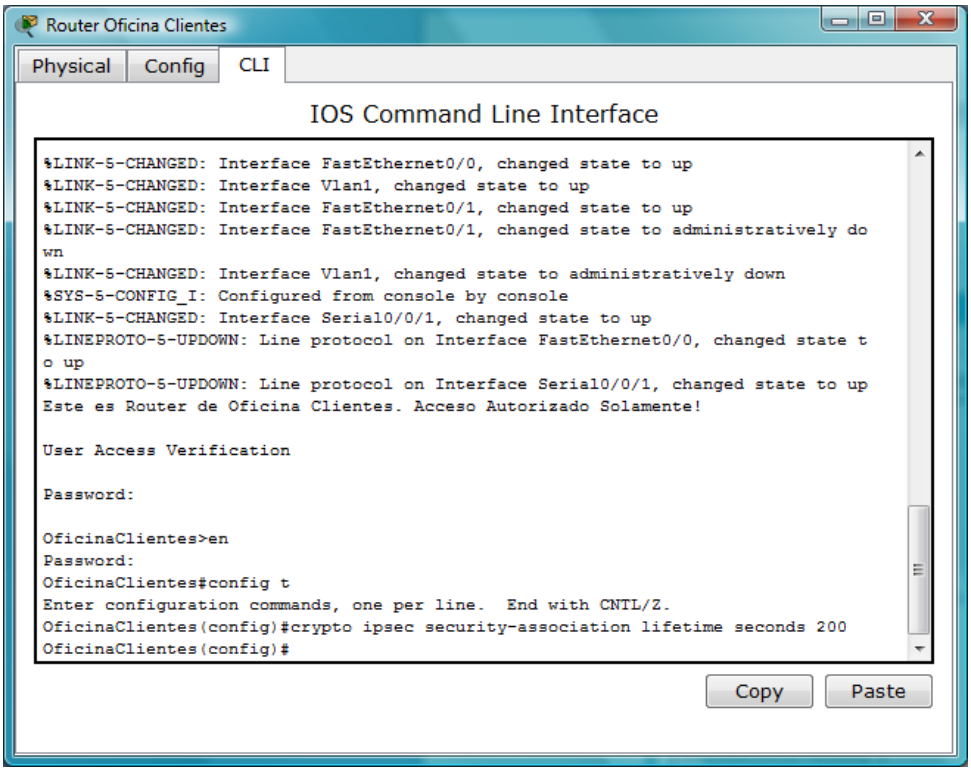


Fuente: Cisco Packet Tracer Versión 5.2

Los tiempos de vida, pueden variar de 120 a 3600 segundos, el tiempo de vida predeterminado para los tiempos de vida de una VPN configurada con IPSec es de 3600 segundos (1 día), esto cuando no se configura ningún tiempo de vida.

[44] Ingeniería del Proyecto. 5.1.3 Configuración de IPSec. 5.1.3.2 Configuración de los tiempos de vida globales de las AS de IPSec con el comando crypto ipsec security-association lifetime.

Figura 27. Configuración del tiempo de vida de la AS del router oficina clientes

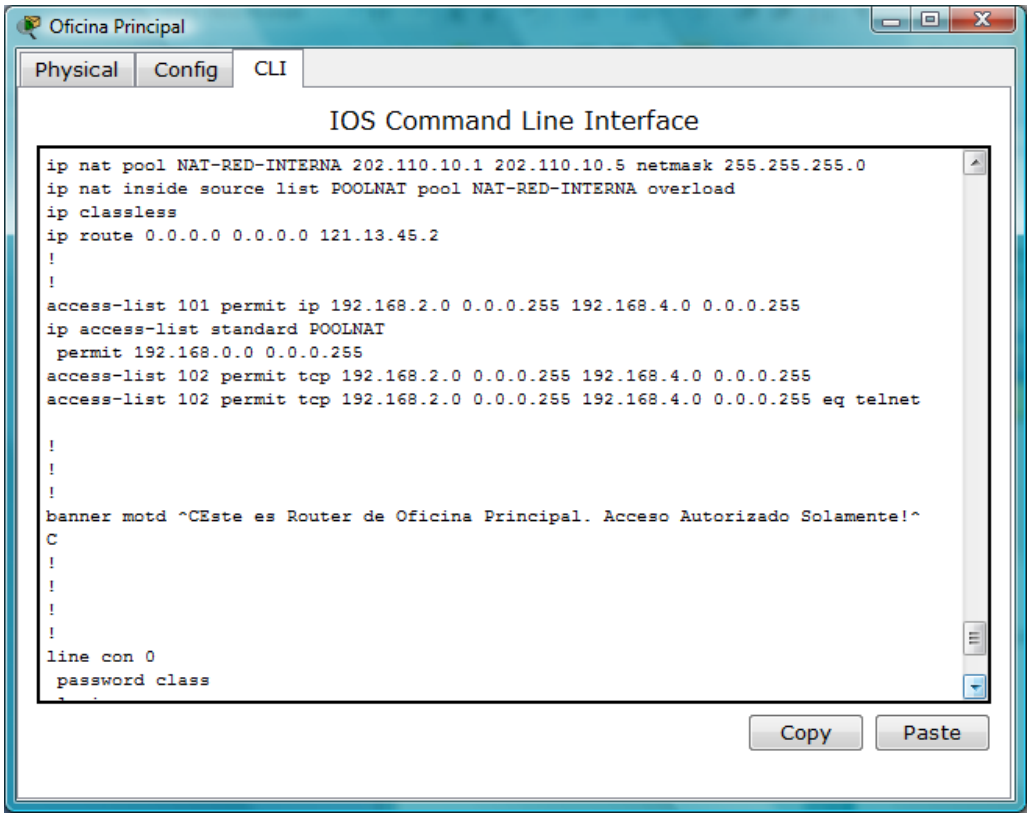


Fuente: Cisco Packet Tracer Versión 5.2

Para permitir que trafico es el que va a fluir libremente en el túnel, una vez se ha establecido la configuración, se deben crear una Lista de Acceso (ACL), esto con el ánimo de indicar el flujo de datos que debe proteger IPSec, seleccionar el trafico externo que debe proteger IPSec.[45]

[45] Ingeniería del Proyecto. 5.1.3 Configuración de IPSec. 5.1.3.3 Configurar las ACL de cifrado con el comando access-list

Figura 28. Creación de Listas de Acceso router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

En el caso de estudio se creó una lista de acceso, la cual nos permite seleccionar el trafico externo que va a ingresar a la VPN, en este caso debido a que los dos routers, se conectan a internet a través de un Proveedor de Servicios, se creó un pool NAT[46] de direcciones llamado NAT-RED-INTERNA, que va desde la dirección 202.110.10.1 a la dirección 202.110.10.5

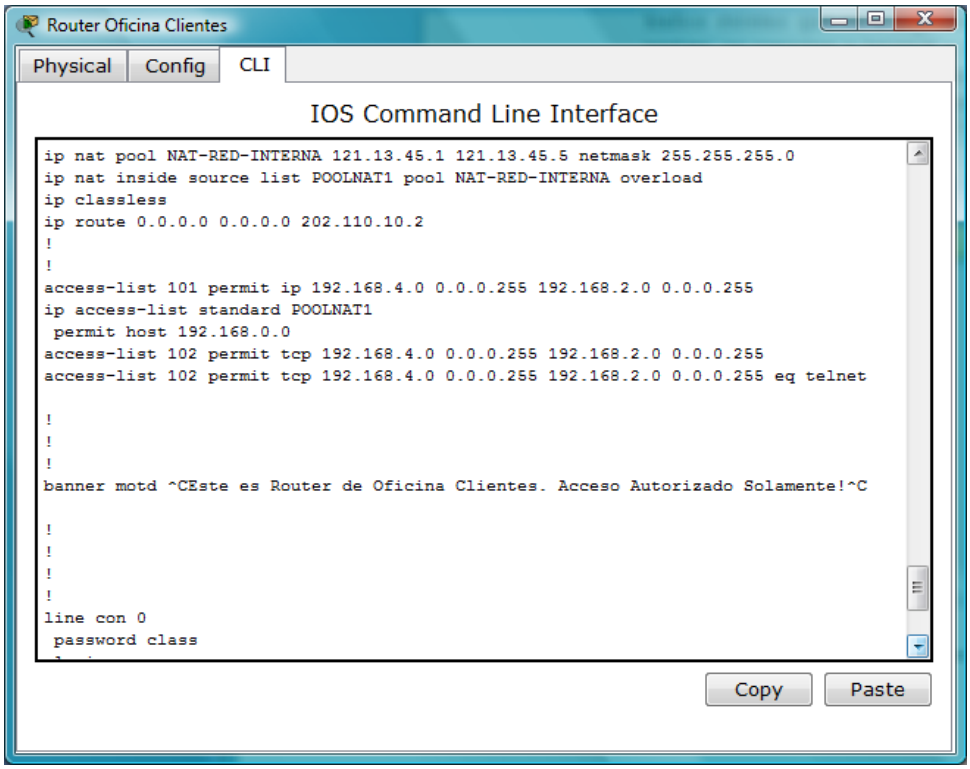
Este pool de direcciones publicas hacen la traducción de direcciones de privada a publica, por tal motivo se crea una lista de acceso que se llama POOLNAT, este pool de direcciones es todo el direccionamiento IP privado que tiene la red empresarial, que en este caso sería el direccionamiento 192.168.2.0 de la red de la oficina principal y el direccionamiento 192.168.4.0 de la red de la oficina de clientes.

La lista de acceso me permite el flujo de datos por protocolo TCP y equivalente a telnet.

[46] NAT (Network Address Translation) permite a direcciones IP privadas salir a Internet por medio de direcciones IP publicas

Lo que en este caso me permitiría poder administrar los routers de la red a través de consola o telnet sin ningún inconveniente, lo que le daría al administrador de la red una mayor seguridad al querer conectarse a cualquiera de los dos routers de forma remota.

Figura 29. Creación de Listas de Acceso router oficina clientes



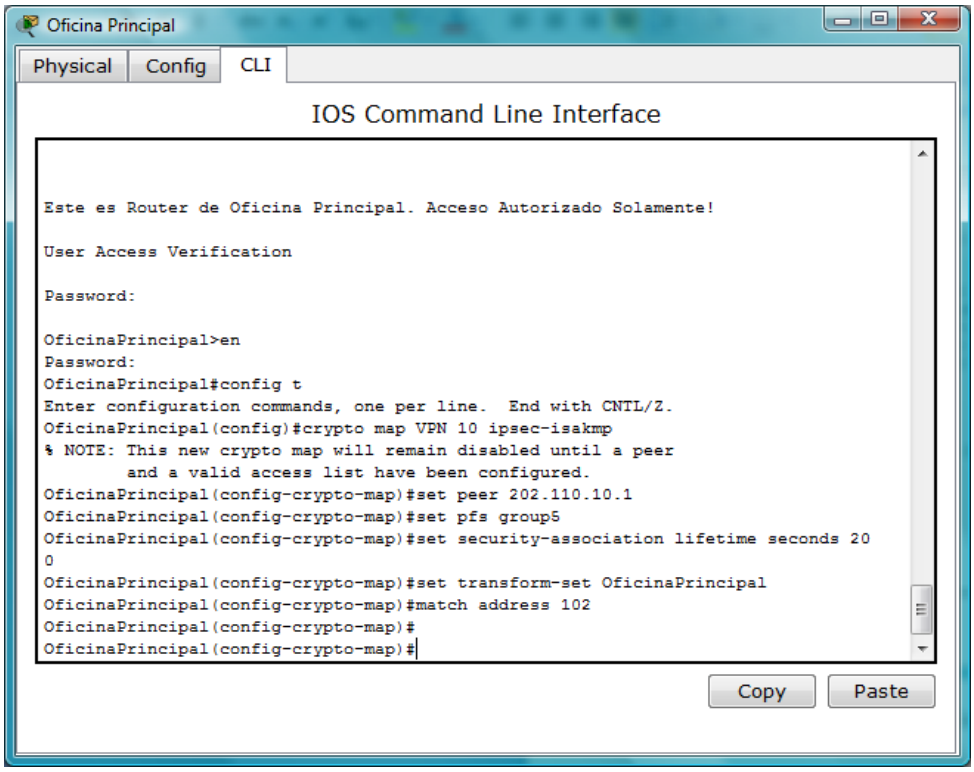
Fuente: Cisco Packet Tracer Versión 5.2

El siguiente paso es la creación de los mapas de cifrado en cada uno de los routers que van a conformar la VPN. Esto con el fin de configurar las Asociaciones de Seguridad para los flujos de datos que se deben cifrar.

Estos mapas de cifrado se pueden configurar solamente a una única interfaz. El comando utilizado para esta configuración es el comando *crypto map*[47]

[47] Ingeniería del Proyecto. 5.1.3 Configuración de IPSec. 5.1.3.4 Configurar los mapas de cifrado con el comando crypto-map

Figura 30. Configuración Mapa de Cifrado router oficina principal



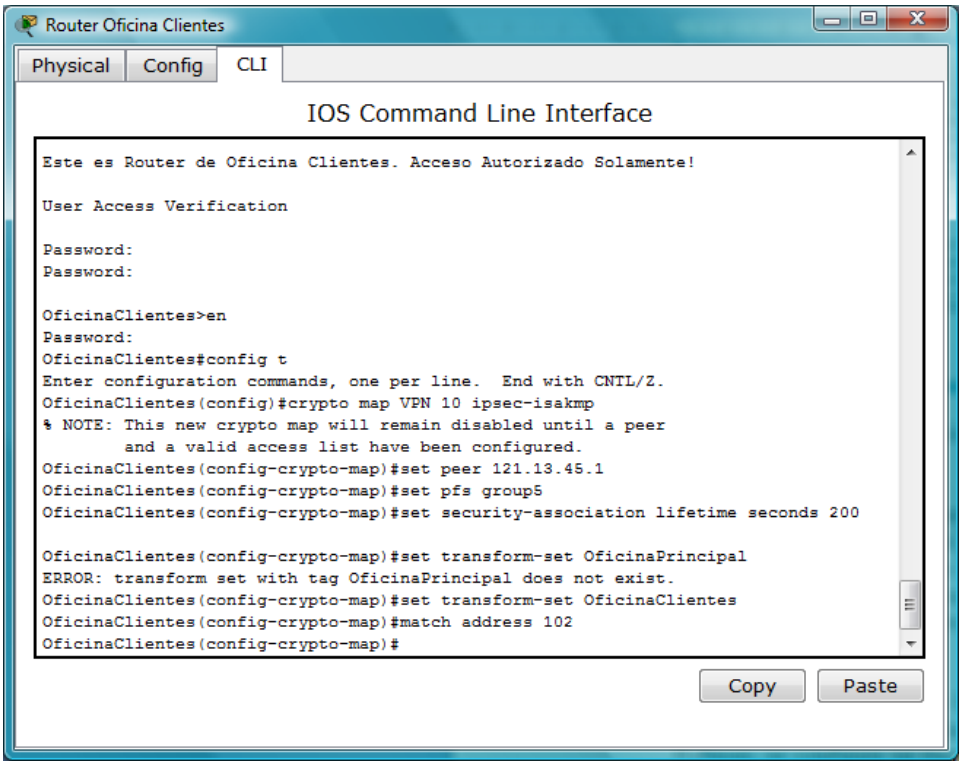
Fuente: Cisco Packet Tracer Versión 5.2

Como se muestra en la Figura 30 se crea un mapa de cifrado con el comando *crypto map* el cual se nombra VPN y se le da un numero de secuencia el cual es el 10, este numero de secuencia asigna la entrada al mapa de cifrado y la instrucción *ipsec-isakmp* Indica que se usara ISAKMP para establecer las Asociaciones de Seguridad de IPSec para proteger el trafico especificado por esta entrada del mapa de cifrado.

Se selecciona un par, que es la dirección IP del router de siguiente salto, que en este caso es el router de oficina clientes. *Set pfs group5* específica el grupo Diffie-Hellman, se configura un tiempo de vida de 200 segundos para la Asociación de Seguridad. El comando *set transform-set OficinaPrincipal* específica la lista de conjuntos de transformación, en este caso el conjunto de transformación que se configuro para este router.

Match Address 102 identifica la ACL, por su nombre o por su número, en este caso, la lista de acceso para la VPN se nombro con el numero 102.

Figura 31. Configuración Mapa de Cifrado router oficina clientes



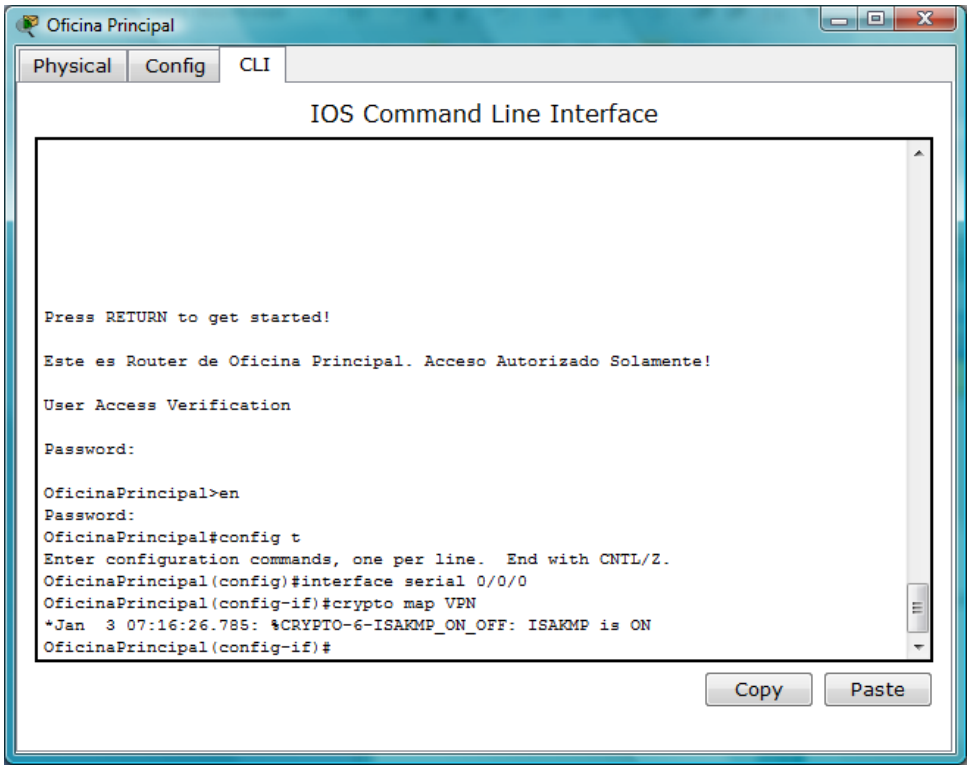
Fuente: Cisco Packet Tracer Versión 5.2

El mismo procedimiento se debe realizar en el router de la oficina de clientes.

El último paso para finalizar la configuración de la VPN es asignar el mapa de cifrado a las interfaces de salida de los routers.[48]

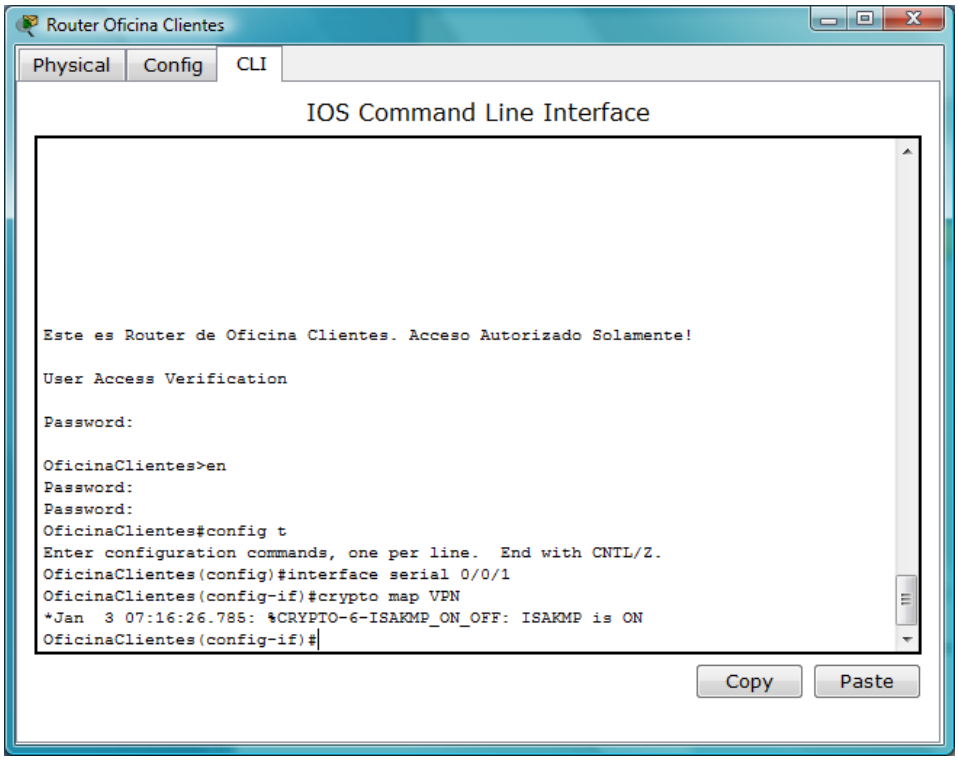
[48] Ingeniería del Proyecto. 5.1.3 Configuración de IPSec. 5.1.3.5 Aplicar los mapas de cifrado a las interfaces de destino o de origen.

Figura 32. Asignación del mapa de cifrado a la interfaz serial de salida



Fuente: Cisco Packet Tracer Versión 5.2

Figura 33. Asignación del mapa de cifrado a la interfaz serial de salida



Fuente: Cisco Packet Tracer Versión 5.2

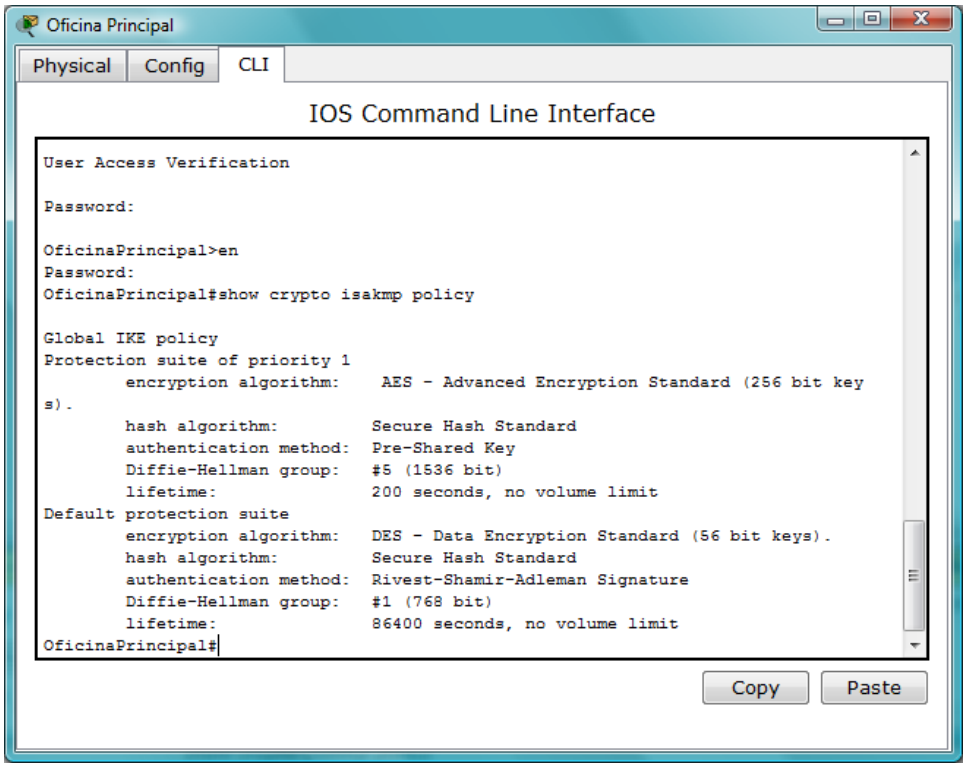
El mismo proceso se realiza a la interfaz serial del router de la oficina clientes.

Hasta este punto el proceso de configuración de la VPN ha finalizado, resta hacer las verificaciones y las comprobaciones de que la configuración está funcionando correctamente.

El primer paso para realizar la verificación de la configuración es revisar los parámetros de cada norma ISAKMP configurada, para esto se utiliza el comando *show crypto isakmp policy*[49]

[49] Ingeniería del Proyecto. 5.1.4 Comprobación y verificación de IPSec.

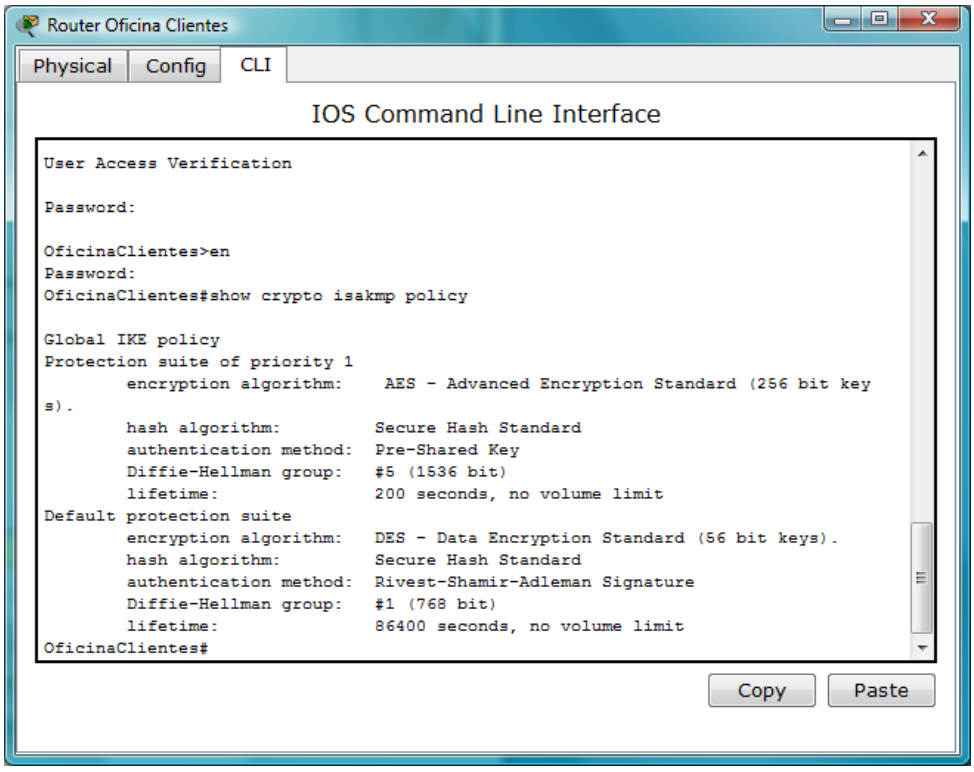
Figura 34. Comprobación de la norma ISAKMP router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

Se verifica que en el router de la oficina de clientes la configuración de la norma ISAKMP sea la misma que en el del router de la oficina principal.

Figura 35. Comprobación de la norma ISAKMP router oficina clientes



Fuente: Cisco Packet Tracer Versión 5.2

Con esta primera verificación se está comprobando que ambos routers tienen la misma configuración de norma ISAKMP.

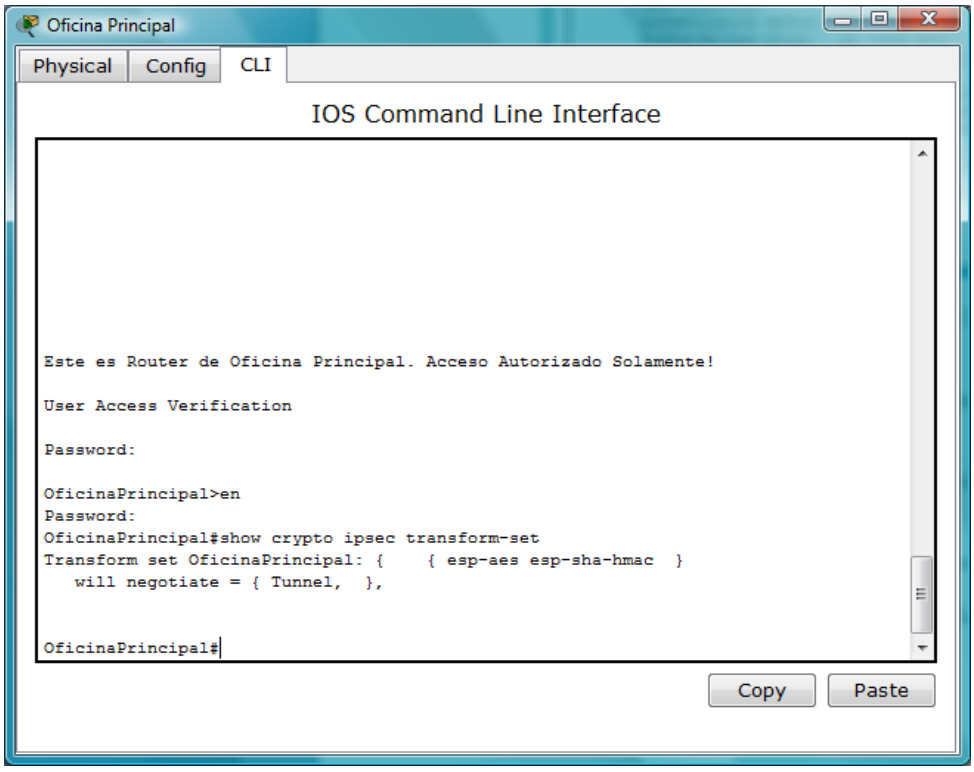
El siguiente paso en la verificación es revisar la correcta configuración de los conjuntos de transformación.

Para verificar esto se utiliza el comando *show crypto ipsec transform-set*

Se debe realizar tanto en el router de la oficina principal como en el router de la oficina de clientes.[50]

[50] Ingeniería del Proyecto. 5.1.4 Comprobación y verificación de IPSec.

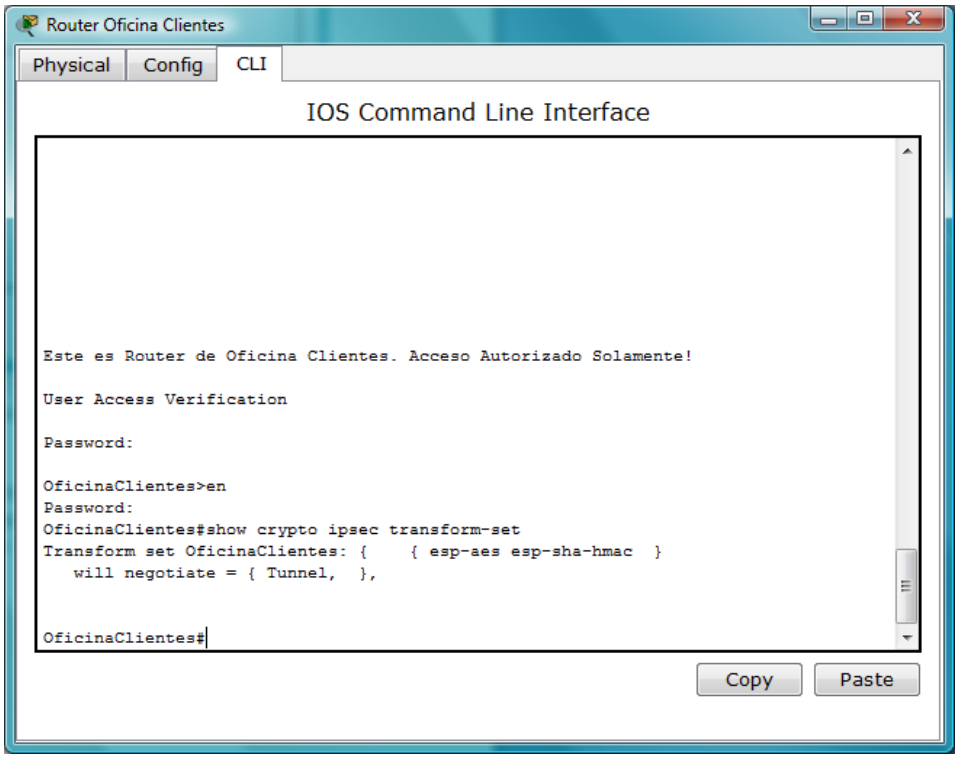
Figura 36. Comprobación de los conjuntos de transformación



Fuente: Cisco Packet Tracer Versión 5.2

Este comando muestra los conjuntos de transformación configurados previamente en el router oficina principal, y muestra el conjunto de autenticación y cifrado *esp-aes esp-sha-hmac* respectivamente, así como la forma en la que se negociara esta Asociación de Seguridad, en este caso *Tunnel*

Figura 37. Comprobación de los conjuntos de transformación

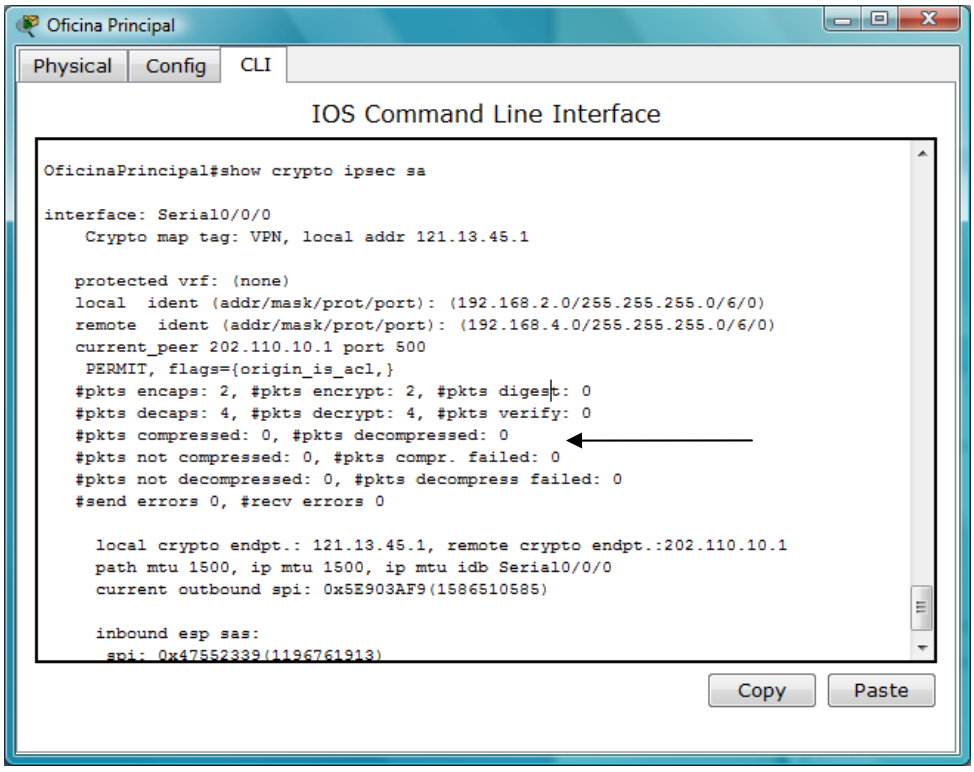


Fuente: Cisco Packet Tracer Versión 5.2

Ahora se debe comprobar las Asociaciones de seguridad entre los dos routers, para esto se utiliza el comando *show crypto ipsec sa.*[51]

[51] Ingeniería del Proyecto. 5.1.4 Comprobación y verificación de IPSec.

Figura 38. Verificación de las Asociaciones de seguridad

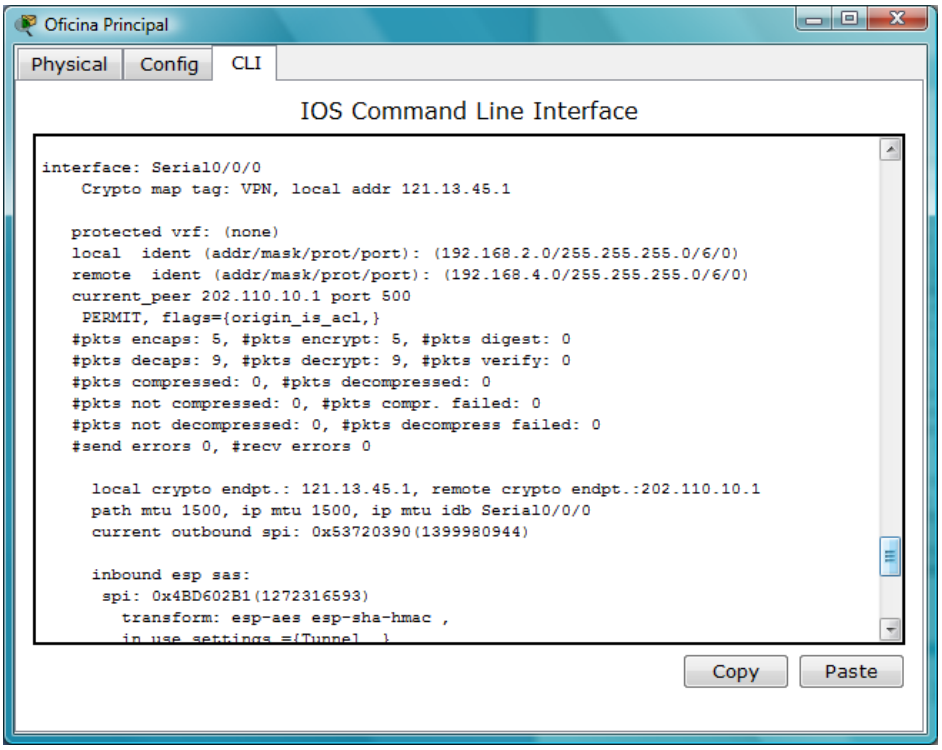


Fuente: Cisco Packet Tracer Versión 5.2

Como se puede observar en la Figura 38, donde la flecha indica en el pantallazo, se han encapsulado 2 paquetes, se han encriptado 2, esto se debe a que desde el computado de la oficina de clientes, se ha accesado al router de la oficina principal a través de telnet.

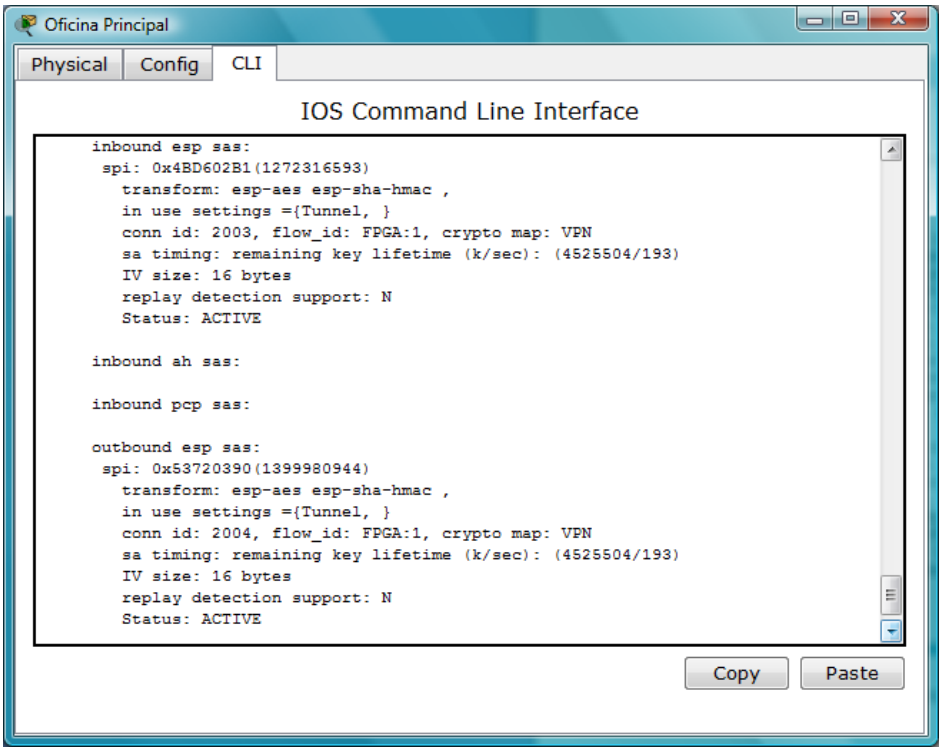
También se realizo un acceso a la página web del servidor de la oficina principal desde el computador de la oficina clientes.

Figura 39. Asociación de Seguridad, acceso a la página web del servidor



Fuente: Cisco Packet Tracer Versión 5.2

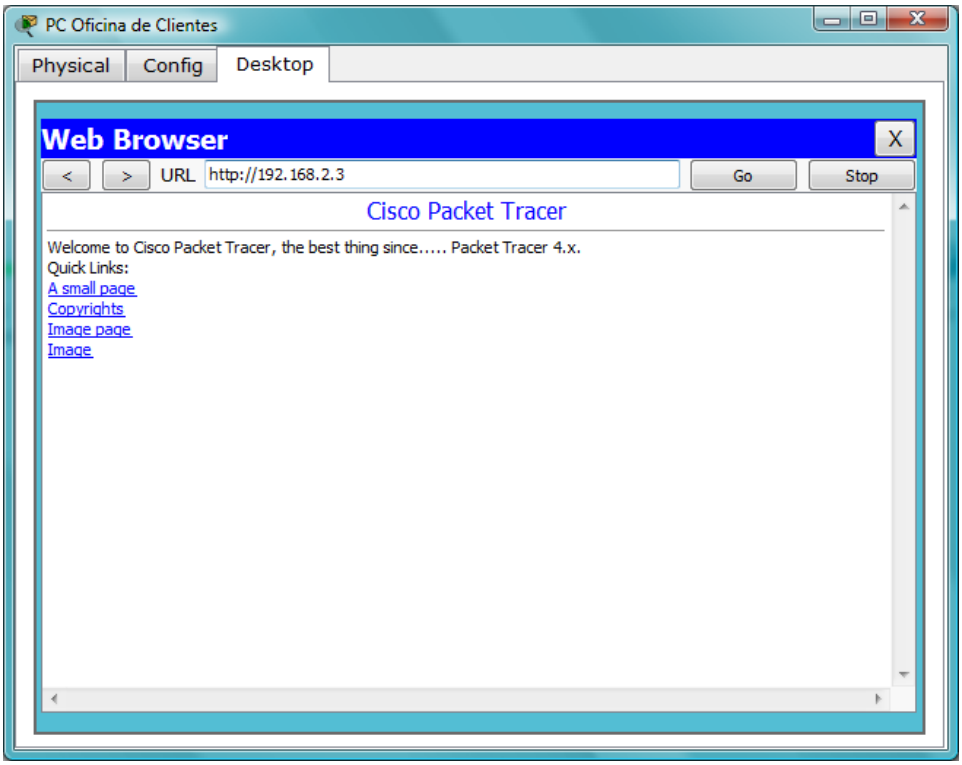
Figura 40. Verificación de Autenticación y Encripción



Fuente: Cisco Packet Tracer Versión 5.2

En la figura 40 se verifica que la autenticación y la encripción de los conjuntos de transformación están en estado ACTIVE

Figura 41. Acceso a la página web del servidor desde computador oficina clientes

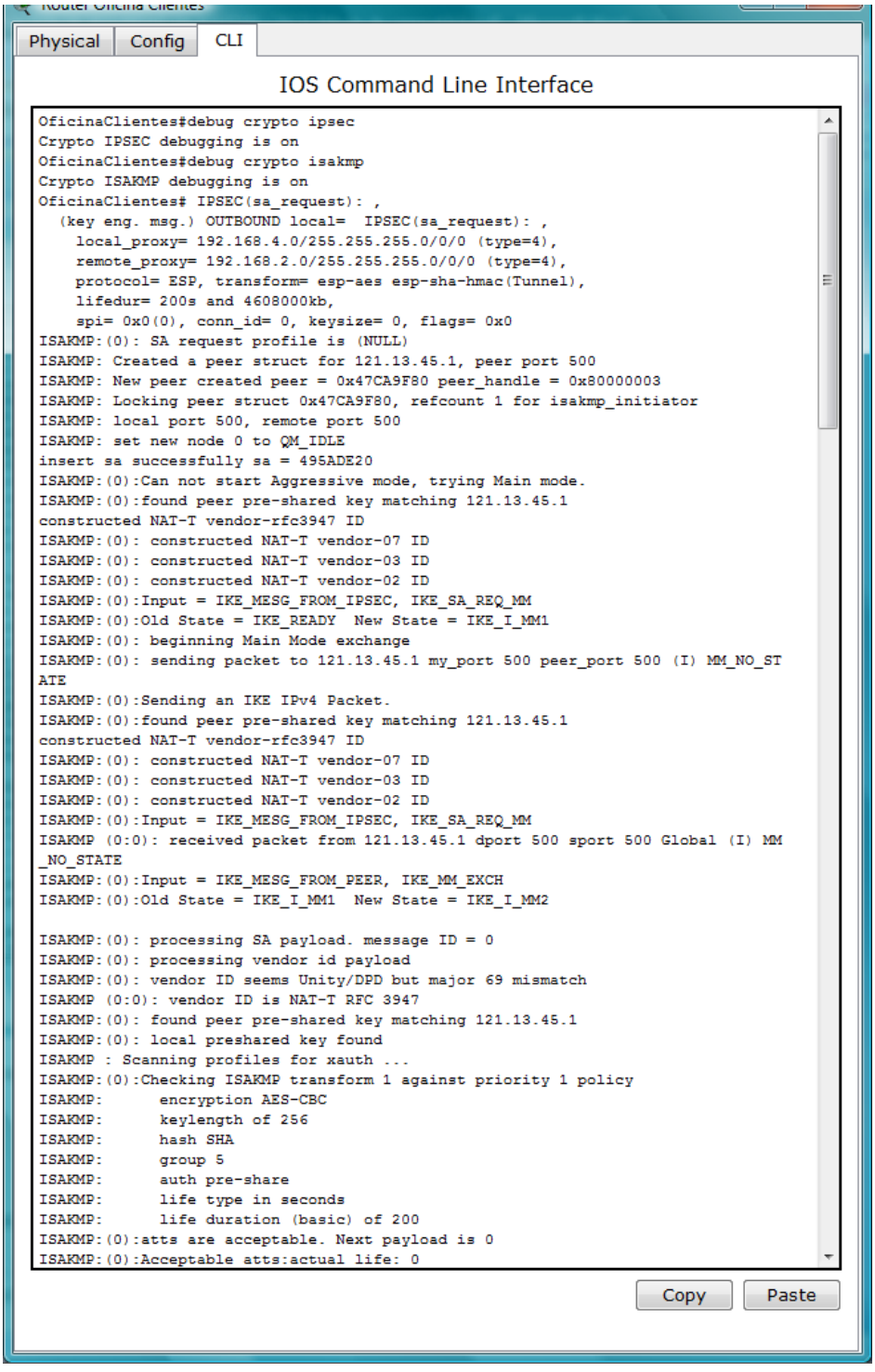


Fuente: Cisco Packet Tracer Versión 5.2

La ultima verificación es verificar los eventos IPSec e ISAKMP, para esto se utilizan los comandos *debug crypto ipsec* y *debug crypto isakmp*[52]

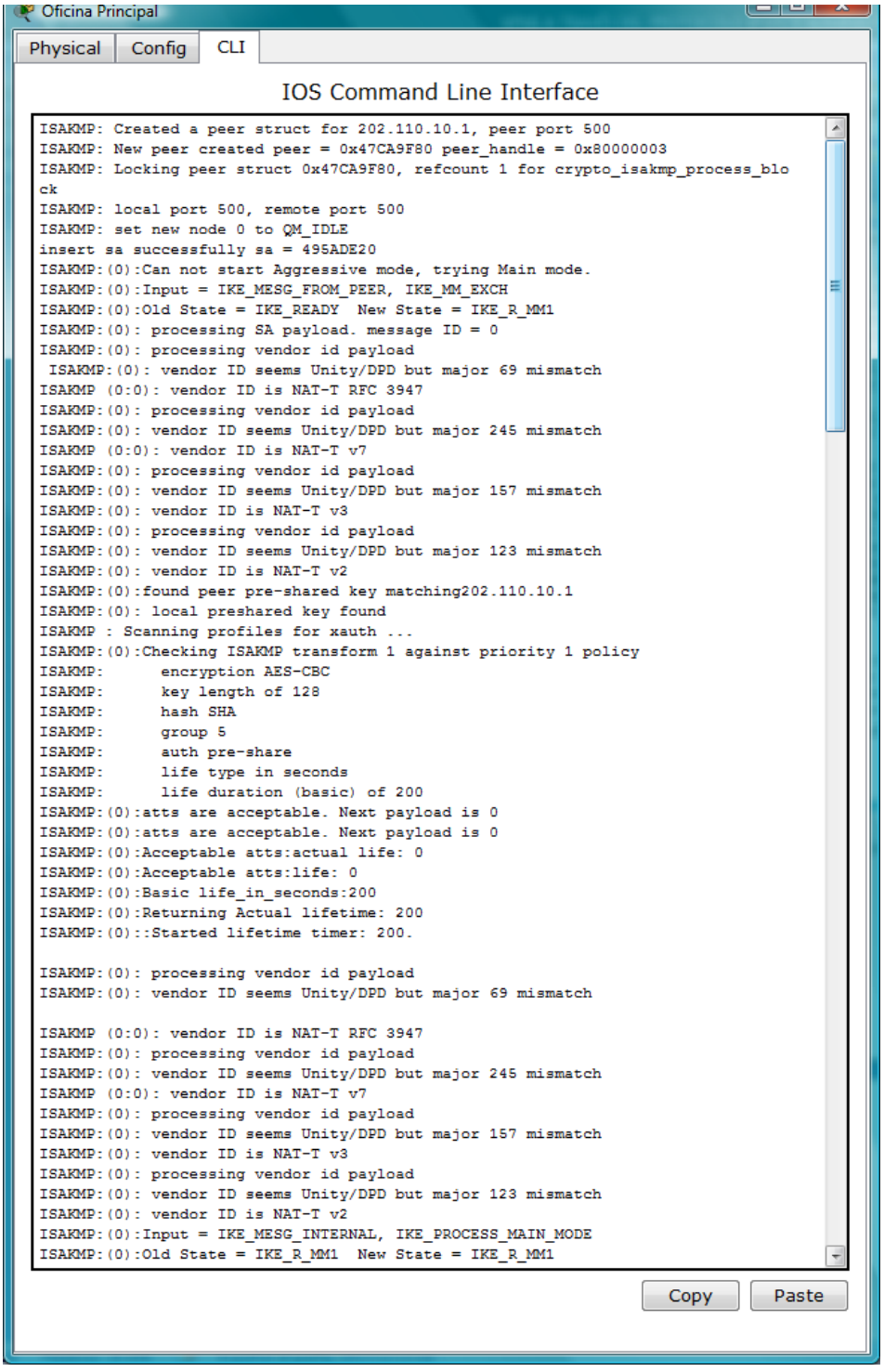
[52] Ingeniería del Proyecto. 5.1.4 Comprobación y verificación de IPSec.

Figura 42. Eventos IPSec e ISAKMP en router oficina clientes



Fuente: Cisco Packet Tracer Versión 5.2

Figura 43. Eventos IPSec e ISAKMP en router oficina principal



Fuente: Cisco Packet Tracer Versión 5.2

6.4 PRACTICA DE LABORATORIO SALON DE HARDWARE Y REDES VPNS POR MEDIO DE PROTOCOLO IPSEC

Una vez realizado el caso de estudio en Packet Tracer, este se verifico y se puso a prueba arrojando unos resultados positivos, las pruebas de conexión de la VPN fueron satisfactorias y el funcionamiento de esta fue correcto.

Se procedió a realizar una practica de laboratorio con computadores y routers reales en el laboratorio de Hardware y Redes de la universidad, para esta practica se utilizaron dos computadores Dell-Optiplex, tres routers marca Cisco modelo 1800 prestados por el monitor de laboratorio, junto a dos cables seriales, dos cables de red, dos cables de poder y un cable de consola, esto con el fin de simular el mismo escenario que se propuso en el caso de estudio.

Figura 44. Routers 1841 Laboratorio Hardware y Redes

Fuente: Laboratorio Hardware y Redes Universidad Libre 2010

Figura 45. Computadores Dell-Optiplex y Cables Seriales Laboratorio Hardware y Redes

Fuente: DELL Computers & Cisco Systems

En esta práctica de laboratorio se dispuso la misma configuración que en el caso de estudio.

Se verifico la configuración de los 3 routers, los cuales se resetearon y se dejaron sin ninguna configuración previa, para comenzar desde cero con la practica y no tener ningún inconveniente.

Una vez conectados los routers por medio de cable serial, se conectaron los dos routers de extremo, en este caso el router que haría de router de Oficina Principal y el Router de extremo que haría de Router de Oficina Clientes, en medio de estos dos routers había otro mas que cumpliría su función como ISP, el cual tendría solo configuradas sus dos interfaces seriales, la Interfaz S 0/0/0 y la Interfaz S 0/0/1, este equipo se le configura una ruta dinámica por medio de protocolo de enrutamiento RIP versión 2.

Al router de Oficina principal se le configuro su interfase FastEthernet 0/0, la cual se conectaría directamente a la Interfaz de Red del computador, y se le configuro la interfase Serial 0/0/0 que conecta directamente con su igual en el ISP, también se configura un enrutamiento dinámico por medio de RIP versión 2 el cual genera una ruta desde la interfaz de red del computador a la internas FastEthernet del Router y una ruta que establece conexión desde la Interfase Serial 0/0/0 del Router Oficina Principal a la Interfase Serial 0/0/0 del ISP.

Para poder acceder al IOS de Cisco y poder configurar los routers era necesario conectar por medio de un cable de consola el router al computador y por medio de HyperTerminal ingresar al router y así poder realizar las configuraciones necesarias, una vez se configuran las direcciones IP de los routers, se configura la IP del computador para que este dentro del mismo direccionamiento del router de extremo, dejando como Gateway la dirección IP de la interfase FastEthernet del Router de extremo, una vez configurado esto ya no era necesario utilizar el cable de consola, sino que se podía trabajar desde el computador conectado al router por medio de un cable de red.

Esta misma configuración se realizo en el otro router de extremo el cual pertenecía a la red de Oficina Clientes.

Para este punto ya se podía realizar una prueba de conectividad desde un router de extremo al otro pasando a través del ISP, por medio de un prueba ping, la cual siempre fue exitosa, confirmando la correcta conectividad entre los routers y los computadores.

Se configuro un NAT en los routers de extremo para que la transmisión de paquetes fuera satisfactoria, ya que ambas redes, Oficina Principal y Oficina Clientes se encontraban de direccionamientos distintos y era necesaria una conexión por medio de NAT para que la transmisión de datos a través del ISP fuera satisfactoria y transparente.

Se configuraron listas de acceso en los routers de extremo para determinar que tipo de tráfico iba a pasar por la VPN, en este caso TCP y Telnet.

Y se configuran listas de acceso para permitir que el tráfico de ambas redes se pueda transmitir sin inconveniente por medio de NAT.

Esta configuración preliminar era la necesaria para que hubiera una conectividad básica entre los equipos, a partir de este punto comenzaría la configuración de la VPN por medio de IPSec, tanto en el router de Oficina Clientes, el ISP y el router de Oficina Principal.

Desafortunadamente no fue posible realizar esta operación y no se pudo continuar con el laboratorio, pues los routers que posee la universidad tienen una imagen de IOS básica, la cual es la IPBASE-MZ-124-3i, la cual solo confiere comandos básicos de conectividad IP, y para poder realizar la configuración de las VPNs era necesario que estos equipos tuvieran la imagen ADVIPSERVICESK9-MZ la cual provee los servicios avanzados de conectividad IP entre ellos IPSec.

RESULTADOS CASO DE ESTUDIO PACKET TRACER

Los resultados de acuerdo con lo descrito demuestran que el protocolo de seguridad de IP IPSec es una de las formas más sencillas, efectivas y seguras de configurar e implementar una VPN en un entorno de red basado en tecnología de CISCO, en este caso dispositivos de capa 3.

Cisco Packet Tracer es un ambiente controlado para la simulación de redes basado en entornos Cisco, por lo tanto los resultados de este caso de estudio fueron positivos, la configuración y la implementación de la VPN se logro satisfactoriamente.

CONCLUSIONES CASO DE ESTUDIO PACKET TRACER

Los objetivos propuestos en la monografía se cumplieron satisfactoriamente, la creación del documento técnico que demuestra la implementación y el funcionamiento de las VPNs a través del protocolo IPSec en entornos de red CISCO se realizo y finalizo en su totalidad, demostrando lo investigado en el caso de estudio diseñado en Packet Tracer.

Se estableció completamente el fundamento teórico y la aplicación de este a la técnica al implementar la VPN en la red del caso de estudio.

Se definió satisfactoriamente como se planifica y se implementa la Administración de la seguridad en los routers cisco.

Como conclusión se puede afirmar que el protocolo de seguridad IP es un protocolo sencillo y seguro que se puede implementar con facilidad en un entorno de red el cual se encuentra correctamente configurado ayudando a este a fortalecer la seguridad, la autenticación y la encripción del flujo de datos que se mueven a través del túnel de la VPN.

RESULTADOS DEL LABORATORIO

El resultado del laboratorio realizado en el laboratorio de Hardware y Redes no fue satisfactorio y no se pudo llevar a cabo en su totalidad, debido a que las imágenes de los routers Cisco 1811 que se encuentran en el laboratorio, vienen con su imagen estándar la cual es la IPBASE MZ-124-3i.

CONCLUSIONES DEL LABORATORIO

El objetivo de esta monografía era demostrar por medio de un documento técnico la implementación y configuración de una VPN por medio del protocolo IPSec, objetivo que se cumple a cabalidad con el caso de estudio objeto de esta investigación, pero este objetivo no se cumple con el laboratorio de practica en Hardware y Redes debido a la carencia de Routers con la imagen apropiada para realizar es configuración.

RECOMENDACIONES

Para que esta práctica sea aplicable como medio de entrenamiento para los siguientes cursos de certificación de CISCO en la Universidad es recomendable que los Routers modelo 1811 que se encuentran en el área de laboratorio de Hardware y Redes tenga una imagen de tipo ADVIPSERVICESK9-MZ, la cual tiene los servicios de configuración de VPNs, ya que la imagen que tienen los routers de laboratorio es la imagen básica IOS IPBASE-MZ-124-3i.

La imagen de servicios avanzados IP permitiría ejecutar prácticas de laboratorio para los cursos de certificación CCNA y CCNP.

En los próximos cursos de certificación en CISCO es recomendable que la frecuencia de las prácticas de laboratorio sean mayores y la teoría solo trate lo básico, la temática de las VPNs se puede tratar más a profundidad en el curso de certificación CISCO CCNA.

A nivel académico se debe profundizar en el tema de VPNs ya que es una parte fundamental de la implementación en las nuevas tecnologías de virtualización y Cloud Computing (Computación en nube).

BIBLIOGRAFIA

KAEO, Merike, CCIE, 2002. Diseño de Seguridad en Redes. Una guía practica para crear una infraestructura. Cisco Press.

MASON G, Andrew, CCIE, 2002. Redes Privadas Virtuales de Cisco Secure. Planifique, desarrolle y mantenga redes privadas virtuales con el libro oficial CSVPN. Cisco Press.

RICHARDSON, Robert, 2008. CSI Computer Crime & Security Survey.

SYSTEM AND NETWORK ATTACK SYSTEM-NATIONAL SECURITY AGENCY. Router Security Configuration Guide. Principles and guidance for secure configuration of IP Routers, with detailed instructions for Cisco Systems Routers.

INFOGRAFIA

http://www.cisco.com

http://es.wikipedia.org

http://www.ietf.org

http://www.rfc-es.org/rfc/rfc2401-es.txt

http://www.rfc-es.org/rfc/rfc2402-es.txt

http://www.rfc-es.org/rfc/rfc2406-es.txt

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

GLOSARIO

A

Acceso: En informática es el resultado positivo de una autentificación, para que el acceso dure un tiempo determinado.

ACK: (Acuse de recibo) en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

ACL: (Lista de Control de Acceso) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Administración de Red: posiciones laborales en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red. Los administradores de red son básicamente el equivalente de red de los administradores de sistemas: mantienen el hardware y software de la red.

ADSL: (Asymetric Digital Suscriber Line) Línea de Abonado Digital Asimétrica, Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 Km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

AES: (Advance Encryption Standard) Estándar de Cifrado Avanzado. También conocido como Rijndael. El AES es un algoritmo simétrico adoptado como estándar por el gobierno de Estados Unidos, y es el sucesor para el estándar de cifrado de datos (DES, Data Encryption Standard).

AH: (Authentication Header) Protocolo de la familia IPSec utilizado para garantizar la integridad de los datos y la autenticación del Host.

Algoritmo: Secuencia de pasos computacionales que transforman una entrada en una salida. Herramienta computacional para resolver un determinado problema, en el cual, debe estar bien especificada la relación entre la entrada y la salida.

Ámbito: Se le llama al contexto que tiene una expresión o valor dentro de un programa, esto se utiliza con el fin de ocultar información, de esta forma la accesibilidad de una variable puede llegar a variar dentro de un mismo programa.

Análogo: Sistema basado en impulsos electromagnéticos que dan origen a una onda. La calidad depende del medio y la frecuencia de uso del material.

Anycast: Forma de direccionamiento en la que la información es enrutada al mejor destino desde el punto de vista de la topología de la red.

Aplicación: Tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo.

ARP: (Address Resolution Protocol) Protocolo de Resolución de Direcciones. Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

ARPA: (Advance Research Project Agency) Agencia de Proyectos de Investigación Avanzada. Se trata del organismo que creó ARPAnet. Creado a instancias del presidente norteamericano Dwight Eisenhower, para hacer frente a la URSS en la carrera espacial. Pero, poco a poco, esta agencia orientó su campo de investigación hacia las telecomunicaciones y las redes informáticas. Precursora de Internet.

Arquitectura de Hardware: Representación de un sistema de hardware electromecánico o electrónico desarrollado o a desarrollar. La arquitectura de hardware primero se concentra en las interfaces eléctricas internas entre los componentes o subsistemas del sistema, y luego la interfaz entre el sistema y su entorno.

Asociación de Seguridad: (SA) es el establecimiento de los atributos compartidos de seguridad entre dos entidades de red para apoyar la comunicación segura.

ATM: (Modo de Transferencia Asíncrona) es una tecnología de telecomunicaciones desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

B

Backbone: Principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante conexiones de fibra óptica. Cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

Base de Datos: Grupo de archivos relacionados. Las bases de datos informatizadas facilitan un rápido acceso a la información necesaria para la toma de decisiones.
Bit: Acrónimo de Binary digit. (Dígito binario). Un bit es un dígito del sistema de numeración binario.

Bootp: (Bootstrap Protocol) Protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente.

BRI: (Basic Rate Interface): Interface básico de acceso en la RDSI que posibilita que coexistan dos canales, uno a 64 kbit/s y otro D a 16 Kbit/s.

Broadcast: Modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Byte: Unidad de información compuesta de 8 bits.

C

Cabecera: Información suplementaria situada al principio de un bloque de información que va a ser almacenada o transmitida y que contiene información necesaria para el correcto tratamiento del bloque de información.

CCNA: plan de capacitación en tecnología de redes que la empresa Cisco ofrece. Se divide en tres niveles, de menor a mayor complejidad: Cisco Certified Network Associate, Cisco Certified Network Professional y Certificado Cisco Experto en Internet.

CD (Compact Disk) Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos).

CDP: (Cisco Discovery Protocol) Protocolo de Descubrimiento de Cisco, es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP.

Cifrar: Escribir un mensaje en clave.

Cisco: Empresa multinacional con sede en San José (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.

Clase: Construcción que se utiliza como un modelo (o plantilla) para crear objetos de esa clase. Este modelo describe el estado y el comportamiento que todos los objetos de la clase comparten.

CPU: (Central Processing Unit) Microprocesador, es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

D

Dato: Representación simbólica (numérica, alfabética, algorítmica etc.), un atributo o una característica de una entidad.

DES: (Data Encryption Standard) Algoritmo para el cifrado de datos, desarrollado por IBM, que utiliza bloques de datos de 64 bits y una clave de 56 bits.
Datagrama: Fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes.

DHCP: (Dinamic Host Configuration Protocol) Protocolo de Configuración Dinámica de Host. Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Dirección IP: Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

DMZ (DeMilitared Zone) Zona Desmilitarizada. Área de una red de computadoras que está entre la red de computadoras interior de una organización y una red de computadoras exterior, generalmente la Internet. La zona desmilitarizada permite que servidores interiores provean la red exterior de servicios, mientras protege la red interior de intromisiones.

DNS (Domain Name System) Sistema de Nombres de Dominio. Sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. (Domain Name Server) Servidor de Nombres de Dominio Ordenador que proporciona a través de una base de datos la conversión del nombre de una dirección de Internet en su dirección IP.

Dominio: Es un conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red. Es la parte principal de una dirección en el Web que usualmente indica la organización o compañía que administra dicha página.

E

EEPROM: (Electrically-Erasable Programmable Read-Only Memory) ROM programable y borrable eléctricamente). Es un tipo de memoria ROM que puede ser programada, borrada

y reprogramada eléctricamente, a diferencia de la EPROM que ha de borrarse mediante un aparato que emite rayos ultravioletas. Son memorias no volátiles.

EIGRP: (Enhanced Interior Gateway Routing Protocol) protocolo de encaminamiento híbrido, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

Enrutamiento: Función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entiende por mejor ruta y en consecuencia cuál es la métrica que se debe utilizar para medirla.

ESP: (Encapsulating Security Payload) proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete.

Ethernet: estándar de redes de computadoras de área local con acceso al medio por contienda ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

F

Fast Ethernet: Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).

FDDI: (Fiber Distributed Data Interface) conjunto de estándares para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica.

Firewall: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Frame Relay: Técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

FTP: (File Transfer Protocol) Protocolo de Transferencia de Archivos. Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

G

Gateway: (Puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Gigabit Ethernet: Ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

H

Host: Computadores conectados a la red, que proveen o utilizan servicios a/de ella.

HTTP: (Hypertext Transfer Protocol) protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force.

HTTPS: (Hypertext Transfer Protocol Secure) protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

I

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (USA). Su Comité de Estándares para las Tecnologías Educativas trabaja con el objetivo de desarrollar estándares técnicos, prácticas recomendadas y guías para la implementación informática de sistemas de formación y educación.

IKE: (Internet Key Exchange). IKE establece una política de seguridad compartida y autentica claves para los servicios que requieren claves (por ejemplo, IPsec).

Interfaz: En electrónica, telecomunicaciones y hardware, una interfaz es el puerto (circuito físico) a través del que se envían o reciben señales desde un sistema o subsistemas hacia otros.

Internet: Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

IOS: IOS (Internetwork Operating System) Sistema Operativo de Interconexión de Redes, sistema operativo creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

IP: (Internet Protocol): Se trata del protocolo primario que rige las comunicaciones a través de Internet, y fue concebido por Vint Cerf y Bob Kahn. Se encarga de definir los métodos de direccionamiento y la encapsulación de los paquetes de datos.

IPSec: (Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IPv4: IPv4 es la versión 4 del Protocolo IP (Internet Protocol) versión anterior de IPv6. Ésta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

IPv6: El protocolo Internet versión 6 (IPv6) es una nueva versión de IP (Internet Protocol), definida en el RFC 2460 y diseñada para reemplazar a la versión 4 (IPv4) RFC 791, que actualmente esta implementado en la gran mayoria de dispositivos que acceden a Internet.

ISDN: (Red digital de servicios integrados). (También llamada RDSI) Juego de normas de la transmisión a gran velocidad de información simultánea de voz, datos e información a través de menos canales de los que serían necesarios de otro modo, mediante el uso de la señalización fuera de banda.

ISAKMP: Internet Security Association and Key Management Protocol es un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Está definido en el RFC 2408.

ITU-T: El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios y publica normativa sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial. Con sede en Ginebra

(Suiza) fue conocido hasta 1992 como Comité Consultivo Telefónico y Telegráfico (CCITT).

K

Kilobyte: Unidad de almacenamiento de información cuyo símbolo es el KB y equivale a 103 bytes.

L

LAN: (Local Área Network) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, o con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

LAPB: (Link Access Procedure, Balanced) es un protocolo de nivel de enlace de datos dentro del conjunto de protocolos de la norma X.25. LAPB está orientado al bit y deriva de HDLC.

M

Memoria Flash: Tipo de memoria que puede ser borrada y reprogramada en unidades de memoria llamadas bloques. Su nombre se debe a que el microchip permite borrar fragmentos de memoria en una sola acción, o flash.

MD5: (Message-Digest Algorithm 5) Algoritmo de Resumen del Mensaje 5 es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Multicast: Envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

N

NAT: (Network Address Translation) Traducción de Dirección de Red es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan

mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.

NFS: (Sistema de archivos de red) protocolo de nivel de aplicación. Es utilizado para sistemas de archivos distribuido en un entorno de red de computadoras de área local.

NTP: (Network Time Protocol) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

NVRAM: (Memoria de Acceso Aleatorio no Volátil) es un tipo de memoria de acceso aleatorio que, como su nombre indica, no pierde la información almacenada al cortar la alimentación eléctrica. En los routers se utiliza, para almacenar un archivo de configuración de respaldo/inicio.

O

Octeto: Un octeto siempre se refiere a una cantidad formada exclusivamente por ocho bits.

OSI: El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) es el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

OSPF: (Open Shortest Path First) protocolo de enrutamiento jerárquico de pasarela interior que usa el algoritmo Dijkstra enlace para calcular la ruta más corta posible.

P

Packet Tracer: Herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco CCNA. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

Parámetro: Variable que puede ser recibida por una rutina o subrutina.

PC: (Personal Computer) es una microcomputadora diseñada en principio para ser usada por una sola persona a la vez.

PROM: (Programmable Read-Only Memory) ROM programable. Es una memoria digital donde el valor de cada bit depende del estado de un fusible (o antifusible), que puede ser quemado una sola vez.

Protocolo: Conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Proxy: Programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor Proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

PSK: (Clave pre-compartida) Un método que realiza claves creadas manualmente y estáticas, utiliza el que configura la red inalámbrica para identificarse a un Ordenador PSK. También funciona como encriptación.
Puerto: Interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir. Dicha interfaz puede ser de tipo físico, o puede ser a nivel de software (por ejemplo, los puertos que permiten la transmisión de datos entre diferentes ordenadores).

R

RADIUS: (Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

RAM: (Random-Access Memory) memoria desde donde el procesador recibe las instrucciones y guarda los resultados.

Red: conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a Internet, e-mail, Chat, juegos), etc.

RFC: (Request For Comments) Solicitud de Comentarios. Es el nombre que se da a una serie de normas que definen el protocolo TCP/IP, así como sus documentos relacionados.

RIP: (Routing Information Protocol) Protocolo de Enrutamiento de Información). Es un protocolo de puerta de enlace interna utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

ROM: (Read-Only Memory) memoria de sólo lectura, es la memoria que se utiliza para almacenar los programas que ponen en marcha el ordenador y realizan los diagnósticos.

Router: Direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador

es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

RPC: (Remote Procedure Call) Llamada a Procedimiento Remoto es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

S

SDM: (Security Device Manager) Una herramienta de mantenimiento basada en una interfaz Web desarrollada por Cisco. No es simplemente una interfaz Web. Es una herramienta java accesible a través del navegador.

SHA: (Secure Hash Algorithm) un conjunto de funciones hash diseñado por la Agencia de Seguridad Nacional de los Estados Unidos.

Sistema Operativo: Conjunto de programas de un sistema de cómputo destinado a administrar y compartir sus recursos, así como coordinar todas sus funciones.

SMTP: (Simple Mail Transfer Protocol) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Sniffing: Se trata de dispositivos que permiten al atacante “escuchar” las diversas comunicaciones que se establecen entre ordenadores a través de una red (fí-sica o inalámbrica) sin necesidad de acceder física ni virtualmente a su ordenador.

SNMP: El Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Software: Equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

Spoofing: Técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

SSH: (Secure SHell) intérprete de órdenes segura. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SYN: bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN de una conexión en el procedimiento de establecimiento de tres fases. Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

T

Tabla de Enrutamiento: Documento electrónico que almacena las rutas a los diferentes nodos en una red informática. Los nodos pueden ser cualquier tipo de aparato electrónico conectado a la red.

TACACS+: (Terminal Access Controller Access Control System) Sistema de control de acceso del controlador de acceso a terminales es un protocolo de autenticación remota que se usa para gestionar el acceso (proporciona servicios separados de autenticación, autorización y registro) a servidores y dispositivos de comunicaciones.

TCP/IP: Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia.

TFTP: (Trivial File Transfer Protocol) Protocolo de transferencia de archivos trivial. Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

Teleworker: Telework, e-worker, es un acuerdo de trabajo en el que los trabajadores gozan de flexibilidad en la ubicación y horario de trabajo.

TELNET: (Telecommunication Network) es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

Token Ring: Token Ring es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; actualmente no es empleada en diseños de redes.

U

UDP: (User Datagram Protocol) protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

Unicast: Envío de información desde un único emisor a un único receptor.

USB: (Universal Serial Bus) bus universal en serie. Abreviado comúnmente USB, es un puerto que sirve para conectar periféricos a un ordenador.

V

VLAN: (Virtual LAN, Red de Área Local Virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.

VPN: (Virtual Private Network) es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

W

WAN: (Wide Area Network) Son redes que se extienden sobre un área geográfica extensa.

X

X.25: Estándar UIT-T para redes de área amplia de conmutación de paquetes.

X-WINDOW: (Sistema de ventanas X) es un software que fue desarrollado a mediados de los años 1980 en el MIT para dotar de una interfaz gráfica a los sistemas Unix.